14-2985

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-2985

In the Matter of a Warrant to Search
a Certain E-mail Account Controlled and Maintained
by Microsoft Corporation

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PETITION FOR REHEARING AND REHEARING *EN BANC*

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.
One St. Andrew's Plaza
New York, New York 10007
(212) 637-2200

TIMOTHY HOWARD,
MARGARET GARNETT,
Assistant United States Attorneys,
Of Counsel.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-2985

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA,

Appellee.

PETITION OF THE UNITED STATES OF AMERICA FOR REHEARING AND REHEARING *EN BANC*

Preliminary Statement

On July 14, 2016, this Court issued an opinion in this matter (Carney, C.J., and Bolden, D.J., by designation; Lynch, C.J., concurring) vacating an order holding Microsoft Corporation ("Microsoft") in contempt, and remanding the case to quash a search warrant (the "Warrant"), issued pursuant to Section 2703 of the Stored Communications Act ("SCA"), that required Microsoft to disclose the contents of an email account to the Government. The majority opinion ("Opinion"), written by Judge Carney and joined by Judge Bolden, reached the unprecedented conclusion

that Section 2703 does not authorize courts to issue and enforce warrants to U.S.-based Internet service providers for the disclosure of customer email content that is stored on foreign servers but entirely within the control of the U.S.-based company. Judge Lynch concurred in a separate opinion, although he disagreed with much of the majority's reasoning.

The Opinion rests almost entirely on the erroneous conclusion that the enforcement of the disclosure obligation in the Warrant would be an impermissible extraterritorial application of Section 2703. In contravention of *RJR Nabisco Inc.* v. *European Community*, 136 S. Ct. 2090 (2016), which clarified that the extraterritoriality inquiry proceeds on a provision-by-provision basis, the Opinion conducts almost no analysis of Section 2703 itself. Instead the Opinion relies on the title of the overall statute in which the SCA appears and provisions of the SCA other than Section 2703 in reaching its conclusion that the "focus" of Section 2703 is "privacy." The Opinion further concludes that the physical location of this nebulous privacy interest is in Dublin, Ireland, even though the email account-holder —the ostensible beneficiary of the privacy interest— does not choose the storage location, cannot prevent Microsoft from moving the email content into the United States or indeed anywhere it chooses, and has no means to determine where Microsoft, in its own business interests, has chosen to store the data.

This case plainly involves a "question[] of exceptional importance," Fed. R. App. P. 35(b)(1)(B), because it is significantly limiting an essential investiga-

tive tool used thousands of times a year, harming important criminal investigations around the country, and causing confusion and chaos among providers as they struggle to determine how to comply. The Opinion breaks with over two decades of settled SCA enforcement and compliance, in holding that a U.S.-based company can refuse to use U.S.-based facilities and employees to comply with a court-authorized disclosure warrant, issued upon a showing of probable cause, merely because the company chooses in its sole discretion to store the electronic data sought by the warrant on its own overseas servers. The Opinion's impact is not limited to cases in which targets are, or claim to be, located overseas and in which it is potentially feasible for the United States to obtain content data from authorities in the country where it is stored. Unlike Microsoft, some major providers cannot easily determine where customer data is physically stored, and some store different parts of customer content data in different countries. Major U.S.-based providers like Google and Yahoo! store a customer's email content across an ever-changing mix of facilities around the world. To the extent content is stored abroad by the provider at the moment the warrant is served, the Opinion has now placed it beyond the reach of a Section 2703 warrant, even when the account owner resides in the United States and the crime under investigation is entirely domestic. At least in the case of Google, the information is also currently beyond the reach of a Mutual Legal Assistance Treaty request or any foreign law enforcement authority, because *only* Google's U.S.-based employees can access customer email accounts, regardless of where they are stored;

indeed, Google cannot reliably identify the particular foreign countries where a customer's email content may be stored. Thus, critical evidence of crimes now rests entirely outside the reach of any law enforcement anywhere in the world, and the randomness of where within an intricate web of servers the requested content resides at a particular moment determines its accessibility to law enforcement. Not surprisingly, the Opinion has substantially impaired law enforcement's ability to use a vital tool to investigate and prosecute all types of serious crime—including terrorism, public corruption, cyber-crime, securities fraud, child sexual exploitation, and major narcotics trafficking—and has thus contravened the express will of Congress that disclosure of electronic communications, with the protections of the warrant requirement, be available to aid in criminal investigations. The appeal should be reheard.[1]

Statement of the Case

A. Microsoft's Customer Email Storage Practices

Microsoft is a U.S.-based provider of email services, available to the public without charge. Op. 7. Microsoft stores the contents of a customer's e-mails, in addition to non-content account information, on a network of computer servers. Those servers are housed in roughly 100 datacenters that Microsoft and its subsidiaries op-

---

[1] The Solicitor General has authorized this petition for rehearing and rehearing *en banc*.

erate in, among other places, the United States, Ireland, and approximately 38 other countries. Op. 7-9. Microsoft asserts that it typically stores email content at datacenters located near the physical location identified by the user as his own when subscribing to the service. Op. 8. Once a user provides his purported location, Microsoft typically migrates all the user's content data to the closest Microsoft-owned datacenter, and, where that process results in storage on a server outside the United States, Microsoft maintains only limited non-content information about the account on servers in the United States. Op. 8-9. Microsoft makes no effort to verify the location provided by the customer, and nothing in the Microsoft customer agreement gives the customer any control, or right to control, where Microsoft stores his email content or when Microsoft moves that content into or out of the United States. Microsoft asserts that, following migration, the only way to access and repatriate user data stored in overseas datacenters is for a Microsoft employee to log into a database management program and access the relevant foreign datacenter. Op. 9. Under current Microsoft practices for responding to requests from U.S. law enforcement agencies, that employee is located in Redmond, Washington.

B. Section 2703

Congress enacted Section 2703 in 1986 as part of the Electronic Communications Privacy Act, and substantially revised Section 2703 in 2001 via the PATRIOT Act. *See* Pub. L. 99-508 § 201; Pub. L. 107-56 §§ 209, 210, 212, 220. Section 2703 regulates the pro-

cesses that the Government can use to require providers of electronic communications services to disclose communications. Most relevant here, Section 2703(a) provides that the Government may require a service provider to disclose the content of email communications in electronic storage no longer than 180 days only when the government obtains "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction," 18 U.S.C. 2703(a), which expressly includes "federal courts with jurisdiction over the offense being investigated," 18 U.S.C. 2711(3).

C. Proceedings Below

On December 4, 2013, Magistrate Judge James C. Francis IV in the Southern District of New York, based on a finding of probable cause, issued the Warrant pursuant to Section 2703 to require Microsoft to disclose the contents of an email account and to authorize the Government to search the disclosed material for evidence of international drug trafficking. Op. 9. Microsoft subsequently determined that the content data related to the target email account was stored in its Dublin, Ireland datacenter. Op. 11. Microsoft disclosed all responsive non-content information that was stored on servers located within the United States, but moved to quash the Warrant with respect to email content stored in Dublin. Op. 11.

Judge Francis denied the motion to quash the Warrant. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014). Judge

Francis noted that he had previously found probable cause for the requested search and, inasmuch as a Section 2703 warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the [Internet Service Provider] to search its servers and seize the e-mail account in question." *Id.* at 471. Accordingly, Judge Francis determined that Congress intended that Section 2703's warrant provision impose similar obligations to a subpoena to "produce information in [the provider's] possession, custody, or control regardless of the location of that information." *Id.* at 472 (citing *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir. 1983)). Judge Francis concluded that Microsoft was obligated to disclose the content information for the target email account, regardless of where it was stored. In the course of his analysis, Judge Francis treated the place where the government would receive and review the disclosed content (the United States), and not the place of storage (Ireland), as the relevant location. *See id.*

Microsoft appealed the decision to then-Chief District Judge Loretta A. Preska, who adopted Judge Francis' reasoning and affirmed. Op. 12.

D. The Opinion

The Panel reversed, vacated the contempt order, and remanded for the District Court to quash the Warrant, holding that enforcing the Warrant would constitute an impermissible extraterritorial application of the statute.

First, relying largely on *RJR Nabisco, Inc.* v. *European Community*, 136 S. Ct. 2090 (2016), and *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247 (2010), the Court held, "with relative ease" and in line with the Government's position at oral argument, that Section 2703 does not apply extraterritorially. *See* Op. 21-32 & n.19. The Court rejected the District Court's finding (and the Government's argument) that the warrant provision in Section 2703 was equivalent to compelled disclosure pursuant to subpoena, because Section 2703 has a separate explicit "subpoena" provision for disclosure of non-content subscriber information and because Section 2703 makes specific reference to the procedures for traditional search warrants outlined in Federal Rule of Criminal Procedure 41. Op. 28-29. Although Section 2703 warrants first require disclosure by service providers in order for government agents to perform the authorized search, the Court asserted that such disclosure to the Government was akin to private parties sometimes being required to assist with searches or seizures pursuant to traditional search warrants. Op. 29. Further, the Court distinguished compelled disclosure of overseas records by subpoena under *Marc Rich* from SCA warrant disclosures, based both on the differences between subpoenas and search warrants, and on the fact that, unlike the financial institution in *Marc Rich*, the data was not Microsoft's own data, but rather data for which its customer had a protectable privacy interest and for which Microsoft acted as a caretaker. Op. 30-31.

After concluding that the SCA does not apply extraterritorially, the Court held that requiring Microsoft to disclose email content stored overseas, but

accessed here in the United States, pursuant to a Section 2703 warrant was a prohibited extraterritorial application of the statute. Op. 32-37. It did so by concluding that the "focus" of the SCA was the *privacy* of stored communications, and not *disclosure* to the government, based on the title of the overall statute that created the SCA (the "Electronic Communications Privacy Act"), and the statutory structure, which permits certain disclosures under Section 2703 as exceptions to broader prohibitions in other SCA sections against unauthorized access and disclosures of data stored by internet service providers. Op. 34-37. Given its conclusion that the SCA's focus is on protecting the privacy of stored data, the Court had "little trouble concluding" that because the data at issue was stored in Dublin, the invasion of the customer's privacy interest would occur there, where it would be "seized" by Microsoft as a compelled agent of the government, and thus the execution of the Warrant was an unlawful extraterritorial application of the SCA. Op. 39. The Court explicitly rejected the District Court's conclusion that the SCA only places obligations on the provider to act domestically to retrieve the data and act within the United States (which Microsoft conceded it would do here), because the Court found that the requested data lay within the jurisdiction of a foreign sovereign, and because the District Court's reasoning overlooked the SCA's formal recognition of the service provider as merely the caretaker of the content data that is entrusted to it by its customers. Op. 40.

Judge Lynch concurred in the judgment, writing separately in part to dispute Microsoft's arguments

that the case involved a government threat to individual privacy, as the Government here had complied with the most restrictive privacy-protecting requirements of Section 2703 and the Fourth Amendment by obtaining a warrant from a neutral magistrate based on a showing of probable cause. Conc. Op. 1-2. Judge Lynch emphasized that Microsoft was not arguing that "if the emails sought … were stored on a server" in the United States "there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case." Conc. Op. 3. Rather, "the sole issue" in the case was "whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country." Conc. Op. 4. Judge Lynch also noted that the Government's characterization of the warrant in this case "as [a] domestic, rather than extraterritorial" application of the statute is "far from frivolous," and found "quite reasonable" the Government's argument that the "focus" of Section 2703 "is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested." Conc. Op. 10-12. Ultimately, however, Judge Lynch agreed with the majority's conclusion, based primarily on his view that Congress had never considered factual circumstances like these when it enacted the SCA, and that the strong presumption against extraterritoriality compelled such a conclusion. Conc. Op. 13-16.

ARGUMENT

The Panel Erroneously Concluded that Enforcement of the Warrant Was an Impermissible Extraterritorial Application

A. The "Focus" of Section 2703 is Disclosure, Which Occurs in the United States

The Government does not challenge the Panel's conclusion that the SCA, and Section 2703 in particular, does not apply extraterritorially. However, that does not end the inquiry. As the Supreme Court explained in *RJR*, if a statute does not have extraterritorial effect, the next question is to "determine whether the case involves a domestic application of the statute, and [courts] do this by looking to the statute's 'focus.'" 136 S. Ct. at 2101. "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *Id*. The "focus" inquiry is provision-specific, not on the statute as a whole, such that some provisions of a statute may apply extraterritorially even where other provisions of the same statute do not. *Id*. at 2101-11 (in RICO, certain aspects of 18 U.S.C. § 1962 apply extraterritorially but § 1964(c) does not); *see also Morrison*, 561 U.S. at 263-65.

Applying those principles here, the focus of Section 2703 is plainly disclosure, not privacy. Each of the first three subsections begins with "a governmental entity may require disclosure" or very similar language, and goes on to describe the specific circumstances in which

the Government may require a service provider to disclose electronic communications, including email content, and the procedures the Government must follow. Section 2703(e) also shields service providers from civil liability for disclosing information in response to process under Section 2703. Indeed, the clear purpose of Section 2703, as a whole, is to outline the circumstances in which a customer's privacy interest in the content of their emails must yield to the Government's interests in obtaining those emails through disclosure by the service provider. The Opinion acknowledges as much. *See* Op. 35 ("Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government"). Moreover, Section 2703's title—"Requirements for governmental access," Pub. L. 99-508 (Oct. 21, 1986), amended to "Required disclosure of customer communications or records," Pub. L. 107-56 (Oct. 26, 2001)—further supports the view that the provision's "focus" is disclosure to the Government.[2]

The majority's conclusion that the "focus" of the SCA is "privacy" rests on several faulty premises, in addition to its failure to conduct the "focus" inquiry on

---

[2] The majority noted the *overall statute's* title—"The Electronic Communications Privacy Act"—as support for its conclusion that the "focus" is privacy. *See* Op. 34. But as set forth above, the "focus" inquiry of *Morrison* and *RJR* proceeds provision by provision, and accordingly the title of Section 2703 is far more relevant to ascertaining the section's focus than the title of the statute as a whole.

a provision-specific basis. First, the Opinion essentially ignores the fact (identified repeatedly by Judge Lynch, *see, e.g.,* Conc. Op. 2-3) that all the references to "privacy" in the SCA, *see, e.g.,* Op. 13-14, 33, must be viewed in the context of an understanding—since the nation's founding and certainly in 1986—that a warrant issued by a neutral magistrate based on a showing of probable cause is a recognized and constitutionally-prescribed means of overcoming *any* privacy interest. Indeed, no privacy interest (whether in email content stored by Microsoft, or in a personal diary stored in a bedroom) is protected against such a warrant. Thus any discussion of privacy in the SCA or its legislative history is occurring in the context of the widespread recognition that the limit of privacy is reached where the warrant begins. The majority acknowledges this only in passing, with seemingly no effect on its analysis. Op. 38.

Second, the Opinion weighted heavily, unmoored from any precedent, the notion that Microsoft is the "caretaker" of customer's privacy interests. *See, e.g.*, Op. 31. This "caretaker" argument is not compelling where it is Microsoft who chooses the storage location and not the customer (indeed the customer does not even know where the content is stored), and both Microsoft and the Panel acknowledge that Microsoft would promptly disclose to the Government any customer email content that it chose to store in the United States. It cannot be true that the "focus" of the statutory provision is privacy, but the protection of that privacy interest rests entirely on the profit-driven deci-

sions of a private business, with no choice by or consultation with the owner of the account and the beneficiary of the privacy interest.

Third, the Panel ignored relevant legislative history of Section 2703. In its consideration of legislative history, the Opinion focuses exclusively on the enactment of the SCA in 1986. Op. 37-39. But in 2001, in response to the 9/11 attacks, Congress passed the USA PATRIOT Act, and four separate provisions of that Act revised Section 2703 to ensure that the SCA's disclosure provisions functioned effectively. *See* USA PATRIOT Act of 2001 §§ 209, 210, 212, 220, Pub. L. 107-56, 115 Stat. 272 (2001). That Act (and its amendments to Section 2703) focused on disclosure: its very first clause stated that its purpose was "to enhance law enforcement investigatory tools." Thus, if there was ever any doubt that the focus of Section 2703 is disclosure rather than privacy, the USA PATRIOT Act removes it. The Opinion, which leaves the warrant provisions of Section 2703 fundamentally broken, is inconsistent with that Act.

In short, the "focus" of Section 2703 is disclosure, and that disclosure happens in the United States, when Microsoft discloses the responsive material to the Government.[3] That understanding also comports

---

[3] Judge Lynch's concurring opinion does not directly address this second step of the *Morrison*/*RJR* inquiry, and never squarely identifies what, in his view, is the "focus" of Section 2703, nor whether the relevant conduct occurs in the United States or elsewhere. Rather, his concurrence seems based primarily on his

with the longstanding legal rule that a subpoenaed party subject to the jurisdiction of the district court is required to turn over materials in that party's control, even if the materials are located elsewhere. *See, e.g.*, *Marc Rich*, 707 F.2d at 670; *Hay Group, Inc.* v. *E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) ("'[p]roduction' refers to the delivery of documents, not their retrieval, and therefore 'the district in which the production . . . is to be made' is not the district in which the documents are housed but the district in which the subpoenaed party is required to turn them over").

Moreover, even if the relevant focus were "privacy," the conduct relevant to that focus would still occur in the United States, when Microsoft discloses the content information to the Government or when law enforcement agents search it. The account owner has no

---

view that Congress did not "demonstrate a clear intention to reach situations of this kind in enacting the Act," because situations of this kind did not exist, nor were they foreseeable, in 1986. Conc. Op. 15. But this cannot be the correct analysis. The applicability of federal statutes, with broadly defined terms like "electronic communications," cannot be held hostage to rapid changes in technology, particularly where, as here, Section 2703 warrants were used by the Government, and honored by Microsoft and other service providers without complaint, for the last two decades of rapid development of internet-based and mobile communications platforms, none of which were widely anticipated in 1986.

privacy interest in his emails being stored in Microsoft's Dublin datacenter, as opposed to Microsoft's datacenters in the United States. Indeed, the undisputed record in this case makes clear that the customer has no say in choosing where Microsoft stores his email content, is not told where that email content is stored, and would have no recourse whatsoever—nor even any notice—if Microsoft decided, for its own private business interests and in its sole discretion, to move that email content into or out of the United States. There is no infringement of the customer's privacy interest in his email content based on where Microsoft, at any given moment, chooses to store that content. Rather, the privacy intrusion occurs only when Microsoft turns over the content to the Government, which occurs in the United States. The majority's conclusion that the intrusion instead occurs where Microsoft "accessed" or "seized" the email content, Op. 39, is plainly wrong, because Microsoft could "access" or "seize" the email content on its own volition at any time and move it into the United States, or to China or Russia, or anywhere it chose, and the content would remain under Microsoft's custody and control and the subscriber could not be heard to complain, unless and until the content were disclosed to the Government or another party. This point is amply demonstrated by the concession of both Microsoft and the majority that Microsoft would have to comply with the Warrant if it had chosen (without consulting the subscriber) to move the target email account into the United States, even mere moments before the Warrant was served.

B. The Opinion Contravenes the Will of Congress that Disclosure Be Permitted for Criminal Investigations

Contrary to the suggestion in the Opinion that law enforcement interests were merely peripheral to Congress' purpose in enacting and amending Section 2703, the entirety of Section 2703 is trained on the means by which the Government may require disclosure of electronic communications, whether by demonstrating to a neutral magistrate that there is probable cause to believe the communications contain evidence of a crime, or by proffering "specific and articulable facts showing that there are reasonable grounds to believe that the … information sought [is] relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(a), (d). In contravention of this clear intent, the Opinion allows U.S.-based service providers to frustrate important criminal investigations, whether purposefully or inadvertently, by adopting a business practice of storing email content overseas. In the best case, the Government may be able to obtain this information via the costly, cumbersome and time-consuming process of seeking legal assistance from foreign authorities pursuant to treaties, where available; but in many cases the Government will have no ability to use those means at all. This effect is already harming important criminal investigations, and it has potentially even farther-reaching consequences. Criminals, like most everyone else today, communicate electronically, and thus prosecutors routinely use Section 2703 warrants to require disclosure of information relevant to a

wide array of criminal investigations.[4] The numbers are substantial. For example, in the second half of 2015, Google alone received 3,716 warrants seeking data from a total of 9,412 accounts. *See* Google Transparency Report, *available at https://www.google.com/transparencyreport/userdatarequests/US/#criminal_legal_requests*. Major service providers like Google and Yahoo!, who store different

---

[4] Significant examples of the vital importance of this investigative technique, in this District alone, include *United States* v. *Clarke*, 13 Mj. 0683 (extensive bribery scheme in violation of the Foreign Corrupt Practices Act); *United States* v. *Ross William Ulbricht*, 14 Cr. 68 (KBF) (international narcotics trafficking on the Silk Road internet platform); *United States* v. *Mitsakos*, 16 Mj. 4997 (securities fraud); *United States* v. *Reza Zarrab*, 15 Cr. 867 (RMG) (large-scale evasion of the financial-sanction regime against Iran); *United States* v. *Samia*, 13 Cr. 521 (LTS) (murder for hire); *United States* v. *Le*, 15 Cr. 38 (AJN) (purchase of the dangerous poison ricin and aggravated identity theft); *United States* v. *Li Fangwei*, 14 Cr. 144 (RA) (international arms trafficking); *United States* v. *El-Hanafi*, 10 Cr. 162 (KMW) (material support to terrorist organizations); *United States* v. *Ashe*, 15 Cr. 706 (VSB) (bribery of United Nations officials); *United States* v. *Skelos*, 15 Cr. 317 (KMW) (bribery of New York state senate majority leader); *United States* v. *Seabrook*, 16 Cr. 467 (ALC) (bribery of the head of the NYC correction officer's union); *United States* v. *Pan*, 12 Cr. 153 (RJS) (election fraud).

pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices, are now disclosing only those portions of customer accounts stored in the United States at the moment the warrant is served—even though, at least as to Google, the *only* employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States. Yahoo! has informed the Government that it will not even preserve data located outside the United States in response to a Section 2703 request, thereby creating a risk that data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data. In addition, some providers are apparently unable to tell the Government, in response to Section 2703 disclosure orders, where particular data is stored or whether it is stored outside the United States, further frustrating law enforcement's ability to access such data.

In clear violation of Congress' expectations when enacting and amending Section 2703, the Opinion has created a regime where electronic communication service providers—private, for-profit businesses answerable only to their shareholders—can thwart legitimate and important criminal and national security investigations, while providing no offsetting, principled privacy protections. As Judge Lynch explained, with respect to Microsoft's customers, "[i]t is only *foreign* customers, and those Americans who *say* that they reside abroad, who gain any enhanced protection from the

Court's holding." Conc. Op. 4. Even if the "focus" of Section 2703 is privacy, Congress cannot have intended to give *greater* privacy protections to foreign nationals and those Americans falsely claiming to reside abroad, while engaged in violations of U.S. criminal laws, than to American citizens at home—indeed, any suggestion to the contrary is absurd. Moreover, even as to those first two favored categories of users, their privacy protection is only as strong as Microsoft's desire to protect it—should Microsoft decide for business reasons, or any reason, or no reason, to store the relevant content in the United States, even Microsoft concedes that neither the subscriber nor Microsoft would have a basis to object to Microsoft disclosing the information pursuant to a validly obtained Section 2703 warrant.

Finally, advancing the clear law enforcement mission of Section 2703 does not run afoul of the extraterritoriality concerns identified by the Panel. Insofar as the presumption against extraterritoriality is meant "[m]ost notably … to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries," *RJR*, 136 S. Ct. at 2100, that concern is substantially muted here, where the entity availing itself of Section 2703 is the executive branch of the federal Government—the branch primarily charged with conducting the nation's foreign relations. The United States Government is well-suited to deciding, given the facts and circumstances of a given case, whether the possibility of international friction is outweighed by the law enforcement need to obtain the information. When the United States decides to seek a Section 2703 warrant for information that may be stored abroad, it takes into account the possibility of

"unintended clashes," *Kiobel* v. *Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013), and "unreasonable interference," *F. Hoffman-La Roche Ltd.* v. *Empagran S.A.*, 542 U.S. 155, 164 (2004), with other countries. Thus, unlike litigation between private parties, which presents a heightened risk of creating international tension that the federal government cannot easily control, *see, e.g.*, *RJR*, 136 S. Ct. at 2106, the same concerns are substantially less pronounced where, as here, the Government itself is a party to the proceedings.

CONCLUSION

The petition for panel rehearing or rehearing *en banc* should be granted

Dated: New York, New York
October 13, 2016

Respectfully submitted,

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.

TIMOTHY HOWARD,
MARGARET GARNETT,
Assistant United States Attorneys,
Of Counsel.

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies that this brief exceeds the page limits set by Rules 35(b)(2) and 40(b) of the Federal Rules of Appellate Procedure, but is within the 21-page limit for which the Government is seeking permission in a motion being filed simultaneously with this petition.

PREET BHARARA,
United States Attorney for the Southern District of New York

By: MARGARET GARNETT,
Assistant United States Attorney

ADDENDUM

Add. 1

14-2985
Microsoft v. United States

United States Court of Appeals
FOR THE SECOND CIRCUIT

August Term, 2015

Argued: September 9, 2015 Decided: July 14, 2016

Docket No. 14-2985

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

B e f o r e :

LYNCH and CARNEY, *Circuit Judges*, and BOLDEN, *District Judge*.*

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York (1) denying Microsoft's motion to quash a warrant ("Warrant") issued under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, to the extent that the orders required Microsoft to produce the contents of a customer's e-mail account stored on a server located outside the United States, and (2) holding Microsoft in civil contempt of court for its failure to comply with the Warrant. We

*The Honorable Victor A. Bolden, of the United States District Court for the District of Connecticut, sitting by designation.

Add. 2

conclude that § 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.

REVERSED, VACATED, AND REMANDED.

Judge Lynch concurs in a separate opinion.

E. JOSHUA ROSENKRANZ, Orrick, Herrington & Sutcliffe LLP (Robert M. Loeb and Brian P. Goldman, Orrick, Herrington & Sutcliffe LLP, New York, NY; Guy Petrillo, Petrillo Klein & Boxer LLP, New York, NY; James M. Garland and Alexander A. Berengaut, Covington & Burling LLP, Washington, DC; Bradford L. Smith, David M. Howard, John Frank, Jonathan Palmer, and Nathaniel Jones, Microsoft Corp., Redmond, WA; *on the brief*), *for Microsoft Corporation*.

JUSTIN ANDERSON, Assistant United States Attorney (Serrin Turner, Assistant United States Attorney, *on the brief*), *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Brett J. Williamson, David K. Lukmire, Nate Asher, O'Melveny & Myers LLP, New York, NY; Faiza Patel, Michael Price, Brennan Center for Justice, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Alex Abdo, American Civil Liberties Union Foundation, New York, NY; *for Amici Curiae* Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation, *in support of Appellant*.

Kenneth M. Dreifach, Marc J. Zwillinger, Zwillgen PLLC, New York, NY and Washington, DC, *for Amicus Curiae* Apple, Inc., *in support of Appellant*.

Add. 3

Andrew J. Pincus, Paul W. Hughes, James F. Tierney, Mayer Brown LLP, Washington, DC, *for Amici Curiae* BSA | The Software Alliance, Center for Democracy and Technology, Chamber of Commerce of the United States, The National Association of Manufacturers, and ACT | The App Association, *in support of Appellant*.

Steven A. Engel, Dechert LLP, New York, NY, *for Amicus Curiae* Anthony J. Colangelo, *in support of Appellant*.

Alan C. Raul, Kwaku A. Akowuah, Sidley Austin LLP, Washington, DC, *for Amici Curiae* AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Association, i2 Coalition, and Application Developers Alliance, *in support of Appellant*.

Peter D. Stergios, Charles D. Ray, McCarter & English, LLP, New York, NY and Hartford, CT, *for Amicus Curiae* Ireland.

Peter Karanjia, Eric J. Feder, Davis Wright Tremaine LLP, New York, NY, *for Amici Curiae* Amazon.com, Inc., and Accenture PLC, *in support of Appellant*.

Michael Vatis, Jeffrey A. Novack, Steptoe & Johnson LLP, New York, NY; Randal S. Milch, Verizon Communications Inc., New York, NY; Kristofor T. Henning, Hewlett-Packard Co., Wayne, PA; Amy Weaver, Daniel Reed, Salesforce.com, Inc., San Francisco, CA; Orin Snyder, Thomas G. Hungar, Alexander H. Southwell, Gibson, Dunn & Crutcher LLP, New York, NY; Mark Chandler, Cisco Systems, Inc., San Jose, CA; Aaron Johnson, eBay Inc., San Jose, CA, *for Amici Curiae* Verizon Communications, Inc., Cisco Systems, Inc., Hewlett-Packard Co., eBay Inc., Salesforce.com, Inc., and Infor, *in support of Appellant*.

Add. 4

Laura R. Handman, Alison Schary, Davis Wright Tremaine LLP, Washington, DC, *for Amici Curiae* Media Organizations, *in support of Appellant*.

Philip Warrick, Klarquist Sparkman, LLP, Portland, OR, *for Amici Curiae* Computer and Data Science Experts, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

Owen C. Pell, Ian S. Forrester, Q.C., Paige C. Spencer, White & Case, New York, NY; Edward McGarr, Simon McGarr, Dervila McGarr, McGarr Solicitors, Dublin, Ireland, *for Amicus Curiae* Jan Philipp Albrecht, Member of the European Parliament, *in support of Appellant*.

SUSAN L. CARNEY, *Circuit Judge*:

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York denying its motion to quash a warrant ("Warrant") issued under § 2703 of the Stored Communications Act ("SCA" or the "Act"), 18 U.S.C. §§ 2701 *et seq.*, and holding Microsoft in contempt of court for refusing to execute the Warrant on the government's behalf. The Warrant directed Microsoft to seize and produce the contents of an e-mail account that it maintains for a customer who uses the company's electronic communications services. A United States magistrate judge (Francis, *M.J.*) issued the Warrant on the government's application, having found probable cause to believe that the account was being used in furtherance of narcotics

trafficking. The Warrant was then served on Microsoft at its headquarters in Redmond, Washington.

Microsoft produced its customer's non-content information to the government, as directed. That data was stored in the United States. But Microsoft ascertained that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains in Ireland and to import that data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the Warrant. The magistrate judge, affirmed by the District Court (Preska, *C.J.*), denied the motion to quash and, in due course, the District Court held Microsoft in civil contempt for its failure.

Microsoft and the government dispute the nature and reach of the Warrant that the Act authorized and the extent of Microsoft's obligations under the instrument. For its part, Microsoft emphasizes Congress's use in the Act of the term "warrant" to identify the authorized instrument. Warrants traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas, *see* Fed. R. Crim. P. 41(b), but their authority generally does not extend further.

The government, on the other hand, characterizes the dispute as merely about "compelled disclosure," regardless of the label appearing on the instrument. It maintains that "similar to a subpoena, [an SCA warrant] requir[es] the recipient to deliver records, physical objects, and other materials to the government" no matter where those documents are located, so long as they are subject to the recipient's custody or control. Gov't Br. at 6. It relies on a collection of court rulings construing properly-served subpoenas as imposing that broad obligation to produce without regard to a document's location. *E.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983).

Add. 6

For the reasons that follow, we think that Microsoft has the better of the argument. When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st–century demands for access and speed and their related, evolving expectations of privacy.

Rather, in keeping with the pressing needs of the day, Congress focused on providing basic safeguards for the privacy of domestic users. Accordingly, we think it employed the term "warrant" in the Act to require pre-disclosure scrutiny of the requested search and seizure by a neutral third party, and thereby to afford heightened privacy protection in the United States. It did not abandon the instrument's territorial limitations and other constitutional requirements. The application of the Act that the government proposes — interpreting "warrant" to require a service provider to retrieve material from beyond the borders of the United States —would require us to disregard the presumption against extraterritoriality that the Supreme Court re-stated and emphasized in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010) and, just recently, in *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, 2016 WL 3369423 (June 20, 2016). We are not at liberty to do so.

We therefore decide that the District Court lacked authority to enforce the Warrant against Microsoft. Because Microsoft has complied with the Warrant's domestic directives and resisted only its extraterritorial aspects, we REVERSE the District Court's denial of Microsoft's motion to quash, VACATE its finding of civil contempt, and REMAND the cause with instructions to the District Court to quash the

Add. 7

Warrant insofar as it directs Microsoft to collect, import, and produce to the government customer content stored outside the United States.

BACKGROUND

I. Microsoft's Web-Based E-mail Service

The factual setting in which this dispute arose is largely undisputed and is established primarily by affidavits submitted by or on behalf of the parties.

Microsoft Corporation is a United States business incorporated and headquartered in Washington State. Since 1997, Microsoft has operated a "web-based e-mail" service available for public use without charge. Joint Appendix ("J.A.") at 35. It calls the most recent iteration of this service Outlook.com.[1] The service allows Microsoft customers to send and receive correspondence using e-mail accounts hosted by the company. In a protocol now broadly familiar to the ordinary citizen, a customer uses a computer to navigate to the Outlook.com web address, and there, after logging in with username and password, conducts correspondence electronically.

Microsoft explains that, when it provides customers with web-based access to e-mail accounts, it stores the contents of each user's e-mails, along with a variety of non-content information related to the account and to the account's e-mail traffic, on a network of servers.[2] The company's servers are housed in datacenters operated by it and its subsidiaries.[3]

---

[1] The company inaugurated Outlook.com in 2013 as a successor to Microsoft's earlier Hotmail.com and MSN.com services.

[2] A "server" is "a shared computer on a network that provides services to clients. . . . An Internet-connected web server is [a] common example of a server." Harry Newton & Steve Schoen, Newton's Telecom Dictionary 1084 (28th ed. 2014) ("*Newton's Telecom Dictionary*").

[3] A "datacenter" is "[a] centralized location where computing resources (*e.g.* host computers, servers, peripherals, applications, databases, and network access) critical to an organization are maintained in a highly controlled physical environment (temperature, humidity, etc.)."

Add. 8

Microsoft currently makes "enterprise cloud service offerings" available to customers in over 100 countries through Microsoft's "public cloud."[4] The service offerings are "segmented into regions, and most customer data (*e.g.* email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located." J.A. at 109. Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when subscribing to the service. Microsoft does so, it explains, "in part to reduce 'network latency'"[5]—*i.e.*, delay—inherent in web-based computing services and thereby to improve the user's experience of its service. J.A. at 36–37. As of 2014, Microsoft "manage[d] over one million server computers in [its] datacenters worldwide, in over 100 discrete leased and owned datacenter facilities, spread over 40 countries." *Id.* at 109. These facilities, it avers, "host more than 200 online services, used by over 1 billion customers and over 20 million businesses worldwide." *Id.* at 109.

One of Microsoft's datacenters is located in Dublin, Ireland, where it is operated by a wholly owned Microsoft subsidiary. According to Microsoft, when its system automatically determines, "based on [the user's] country code," that storage for an e-mail account "should be migrated to the Dublin datacenter," it transfers the data associated with the account to that location. *Id.* at 37. Before making the transfer, it

---

Newton's Telecom Dictionary at 373.

[4] The Supreme Court has recently described "[c]loud computing" as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

[5] Microsoft explains network latency as "the principle of network architecture that the greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service." J.A. at 36.

does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol.

Under practices in place at the time of these proceedings, once the transfer is complete, Microsoft deletes from its U.S.-based servers "all content and non-content information associated with the account in the United States," retaining only three data sets in its U.S. facilities. *Id*. at 37. First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." *Id.* Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database. *Id.* at 37–38.

Microsoft asserts that, after the migration is complete, the "only way to access" user data stored in Dublin and associated with one of its customer's web-based e-mail accounts is "from the Dublin datacenter." *Id*. at 37. Although the assertion might be read to imply that a Microsoft employee must be physically present in Ireland to access the user data stored there, this is not so. Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the United States, it can "collect" account data that is stored on any of its servers globally and bring that data into the United States. *Id*. at 39–40.

II. Procedural History

On December 4, 2013, Magistrate Judge James C. Francis IV of the United States District Court for the Southern District of New York issued the "Search and Seizure Warrant" that became the subject of Microsoft's motion to quash.

Add. 10

Although the Warrant was served on Microsoft, its printed boilerplate language advises that it is addressed to "[a]ny authorized law enforcement officer." *Id*. at 44. It commands the recipient to search "[t]he PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation."[6] *Id.* It requires the "officer executing [the] warrant, or an officer present during the execution of the warrant" to "prepare an inventory . . . and promptly return [the] warrant and inventory to the Clerk of the Court." *Id.*

Its Attachment A, "Property To Be Searched," provides, "This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation . . . ." *Id*. at 45. Attachment C, "Particular Things To Be Seized,"[7] directs Microsoft to disclose to the government, "for the period of inception of the account to the present," and "[t]o the extent that the information . . . is within the possession, custody, or control of MSN [redacted]," *id*., the following information:

> (a) "The contents of all e-mails stored in the account, including copies of e-mails sent from the account";
> (b) "All records or other information regarding the identification of the account," including, among other things, the name, physical address, telephone numbers, session times and durations, log-in IP addresses, and sources of payment associated with the account;
> (c) "All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files"; and
> (d) "All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken."

---

[6] The name of the e-mail address associated with the account is subject to a sealing order and does not bear on our analysis.

[7] Although the Warrant includes an Attachment A and C, it appears to have no Attachment B.

Add. 11

J.A. 46–47.[8]

After being served with the Warrant, Microsoft determined that the e-mail contents stored in the account were located in its Dublin datacenter. Microsoft disclosed all other responsive information, which was kept within the United States, and moved the magistrate judge to quash the Warrant with respect to the user content stored in Dublin.

As we have recounted, the magistrate judge denied Microsoft's motion to quash. In a Memorandum and Order, he concluded that the SCA authorized the District Court to issue a warrant for "information that is stored on servers abroad." *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) ("*In re Warrant*"). He observed that he had found probable cause for the requested search, and that the Warrant was properly served on Microsoft in the United States. He noted that, inasmuch as an SCA warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the ISP [Internet service provider] to search its servers and seize the e-mail account in question." *Id.* at 471. Accordingly, he determined that Congress intended in the Act's warrant provisions to import obligations similar to those associated with a subpoena to "produce information in its possession, custody, or control regardless of the location of that information." *Id.* at 472 (citing *Marc Rich*, 707 F.2d at 667). While acknowledging that Microsoft's analysis in favor of quashing the Warrant with respect to foreign-stored customer content was "not inconsistent with the statutory language," he saw Microsoft's position as "undermined by the structure of the SCA, its legislative history,"

[8] The Warrant also describes in Attachment C techniques that would be used (presumably by the government, not Microsoft) "to search the seized e-mails for evidence of the specified crime." J.A. at 47.

and "by the practical consequences that would flow from adopting it." He therefore concluded that Microsoft was obligated to produce the customer's content, wherever it might be stored. He also treated the place where the government would *review* the content (the United States), not the place of *storage* (Ireland), as the relevant place of seizure.

Microsoft appealed the magistrate judge's decision to Chief Judge Loretta A. Preska, who, on *de novo* review and after a hearing, adopted the magistrate judge's reasoning and affirmed his ruling from the bench. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 1:13-mj-02814 (S.D.N.Y. filed Dec. 4, 2013), ECF No. 80 (order reflecting ruling made at oral argument).

Microsoft timely noticed its appeal of the District Court's decision denying the motion to quash. Not long after, the District Court acted on a stipulation submitted jointly by the parties and held Microsoft in civil contempt for refusing to comply fully with the Warrant.[9] *Id.* at ECF No. 92. Microsoft timely amended its notice of appeal to reflect its additional challenge to the District Court's contempt ruling.

We now reverse the District Court's denial of Microsoft's motion to quash; vacate the finding of contempt; and remand the case to the District Court with instructions to

[9] As reflected in their stipulation, Microsoft and the government agreed to the contempt finding to ensure our Court's appellate jurisdiction over their dispute. *See United States v. Punn*, 737 F.3d 1, 5 (2d Cir. 2013) (noting general rule that contempt finding needed before ruling denying motion to quash is sufficiently "final" to support appellate jurisdiction). Because Microsoft timely appealed the contempt ruling, we need not decide whether we would have had jurisdiction over an appeal taken directly from the denial of the motion to quash. *See United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 468–69 (2d Cir. 1996) (noting exception to contempt requirement as basis for appellate jurisdiction in context of third party subpoena issued in administrative investigation).

quash the Warrant insofar as it calls for production of customer content stored outside the United States.

III. Statutory Background

The Warrant was issued under the provisions of the Stored Communications Act, legislation enacted as Title II of the Electronic Communications Privacy Act of 1986. Before we begin our analysis, some background will be useful.

A. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act ("ECPA") became law in 1986.[10] As it is summarized by the Department of Justice, ECPA "updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications."[11] ECPA's Title II is also called the Stored Communications Act ("SCA"). The Act "protects the privacy of the contents of files stored by service

[10] Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848, 1848–73 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701 *et seq.*, and 18 U.S.C. §§ 3121 *et seq.*).

[11] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited May 12, 2016). The Department advises that the acronym "ECPA" is commonly used to refer to the three titles of ECPA as a group (Titles I, II, and III of Pub. L. 99-508). *Id.* Title I "prohibits the intentional actual or attempted interception, use, disclosure, or procurement of any other person" to intercept wire, oral, or electronic transmissions; Title II is the Stored Communications Act, discussed in the text; Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing their installation. *Id.* Title I and III are codified at 18 U.S.C. §§ 2510-22; Title II is codified at 18 U.S.C. §§ 2701-12, and constitutes chapter 121 of Title 18.

providers and of records held about the subscriber by service providers," according to the Justice Department.[12] We discuss its provisions further below.

B. The Technological Setting in 1986

When it passed the Stored Communications Act almost thirty years ago, Congress had as reference a technological context very different from today's Internet-saturated reality. This context affects our construction of the statute now.

One historian of the Internet has observed that "before 1988, the *New York Times* mentioned the Internet only once—in a brief aside." Roy Rosenzweig, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, 103 Am. Hist. Rev. 1530, 1530 (1998). The TCP/IP data transfer protocol—today, the standard for online communication—began to be used by the Department of Defense in about 1980. *See* Leonard Kleinrock, *An Early History of the Internet*, IEEE Commc'ns Mag. 26, 35 (Aug. 2010). The World Wide Web was not created until 1990, and we did not even begin calling it that until 1993. Daniel B. Garrie & Francis M. Allegra, *Plugged In: Guidebook to Software and the Law* § 3.2 (2015 ed.). Thus, a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy. *See* Craig Partridge, *The Technical Development of Internet Email*, IEEE Annals of the Hist. of Computing 3, 4 (Apr.-June 2008).

C. The Stored Communications Act

As the government has acknowledged in this litigation, "[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided by the

[12] *See supra* note 11.

Fourth Amendment." Gov't Br. at 29 (citing S. Comm. on Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541, at 5 (1986)). The SCA provides privacy protection for users of two types of electronic services—electronic communication services ("ECS") and remote computing services ("RCS")—then probably more distinguishable than now.[13] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1213–14 (2004). An ECS generally operated by providing the user access to a central computer system through which to send electronic messages over telephone lines. S. Rep. No. 99-541, at 8. If the intended recipient also subscribed to the service, the provider temporarily stored the message in the recipient's electronic "mail box" until the recipient "call[ed] the company to retrieve its mail." *Id.* If the intended recipient was not a subscriber, the service provider could print the communication on paper and complete delivery by postal service or courier. *Id.*; U.S. Congress, Office of Technology Assessment, OTA-CIT-293, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 47–48 (1985).[14] An RCS generally operated either by providing customers with access to computer processing facilities in a "time-sharing arrangement," or by directly processing data that a customer transmitted electronically to the provider by means of electronic communications, and transmitting back the requested results of particular operations. S. Rep. No. 99-541, at 10–11. We will refer to

[13] *See* 18 U.S.C. § 2510(15) (in ECPA Title I, defining "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); § 2711(2) (in ECPA Title II, the SCA, defining "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

[14] For example, in 1984, Federal Express entered the e-mail market with a service that provided for two-hour delivery of facsimile copies of e-mail messages up to five pages in length. U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, at 47.

Microsoft and other providers of ECS and RCS jointly as "service providers," except where the distinction makes a difference.

As to both services, the Act imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations. Thus, its initial provision, § 2701, prohibits unauthorized third parties from, among other things, obtaining or altering electronic communications stored by an ECS, and imposes criminal penalties for its violation. Section 2702 restricts the circumstances in which service providers may disclose information associated with and contents of stored communications to listed exceptions, such as with the consent of the originator or upon notice to the intended recipient, or pursuant to § 2703. Section 2703 then establishes conditions under which the government may require a service provider to disclose the contents of stored communications and related obligations to notify a customer whose material has been accessed. Section 2707 authorizes civil actions by entities aggrieved by violations of the Act, and makes "good faith reliance" on a court warrant or order "a complete defense." 18 U.S.C. § 2707(e).[15]

Regarding governmental access in particular, § 2703 sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government. Basic subscriber and transactional information can be obtained simply with an administrative subpoena.[16] 18 U.S.C. § 2703(c)(2). Other

[15] Other provisions of the Act address, among other things, preservation of backup data (§ 2704); delaying notice to a customer whose information has been accessed (§ 2705); cost reimbursement for assembling data demanded under the Act (§ 2706); and exclusivity of remedies that the Act provides to a person aggrieved by its violation (§ 2708).

[16] An "administrative subpoena" is "a subpoena issued by an administrative agency to compel an individual to provide information to the agency." *Administrative subpoena*, Black's Law Dictionary (10th ed. 2014). To obtain such a subpoena, the government need not demonstrate probable cause. *See EEOC v. United Parcel Serv., Inc.*, 587 F.3d 136, 139-40 (2d Cir. 2009).

non-content records can be obtained by a court order (a "§ 2703(d) order"), which may be issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." § 2703(c)(2), (d). The government may also obtain some user content with an administrative subpoena or a § 2703(d) order, but only if notice is provided to the service provider's subscriber or customer. § 2703(b)(1)(B). To obtain "priority stored communications" (our phrase), as described below, the Act generally requires that the government first secure a warrant that has been issued "using the procedures described in the Federal Rules of Criminal Procedure," or using State warrant procedures, both of which require a showing of probable cause.[17] Priority stored communications fall into two categories: For

[17] Thus, § 2703, "Required disclosure of customer communications or records," provides in part as follows:

> (a) Contents of wire or electronic communications in electronic storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> (b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

Add. 18

electronic communications stored *recently* (that is, for less than 180 days) by an ECS, the government *must* obtain a warrant. § 2703(a). For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer. § 2703(b)(1)(A).

As noted, § 2703 calls for those warrants issued under its purview by federal courts to be "issued using the procedures described in the Federal Rules of Criminal Procedure." Rule 41 of the Federal Rules of Criminal Procedure, entitled "Search and Seizure," addresses federal warrants. It directs "the magistrate judge or a judge of a state court of record" to issue the warrant to "an officer authorized to execute it." Rule 41(e)(1). And insofar as territorial reach is concerned, Rule 41(b) describes the extent of

---

> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> (ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title. . . .
>
> (g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

the power of various authorities (primarily United States magistrate judges) to issue warrants with respect to persons or property located within a particular federal judicial district. It also allows magistrate judges to issue warrants that may be executed outside of the issuing district, but within another district of the United States. Fed. R. Crim. P. 41(b)(2), (b)(3). Rule 41(b)(5) generally restricts the geographical reach of a warrant's execution, if not in another federal district, to "a United States territory, possession, or commonwealth," and various diplomatic or consular missions of the United States or diplomatic residences of the United States located in a foreign state.

DISCUSSION

I. Standard of Review

We will vacate a finding of civil contempt that rests on a party's refusal to comply with a court order if we determine that the district court relied on a mistaken understanding of the law in issuing its order. *United States ex rel. Touhy v. Ragen*, 340 U.S. 462, 464–70 (1951). Similarly, we will vacate a district court's denial of a motion to quash if we conclude that the denial rested on a mistake of law.[18] *See In re Subpoena Issued to Dennis Friedman*, 350 F.3d 65, 68–69 (2d Cir. 2003).

It is on the legal predicate for the District Court's rulings—its analysis of the Stored Communications Act, in particular, and of the principles of construction set forth by the Supreme Court in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010)—that we focus our attention in this appeal.

---

[18] Our Court has not squarely held what standard governs our review of a district court's denial of a motion to quash and its related contempt finding. We need not dwell long on this threshold question, however, because even a deferential abuse-of-discretion review incorporates a *de novo* examination of the district court's rulings of law, such as we conduct here. *See, e.g., In re Grand Jury Subpoena Issued June 18, 2009*, 593 F.3d 155, 157 (2d Cir. 2010).

Add. 20

II. Whether the SCA Authorizes Enforcement of the Warrant as to Customer Content Stored in Ireland

A. Analytic Framework

The parties stand far apart in the analytic frameworks that they present as governing this case.

Adopting the government's view, the magistrate judge denied Microsoft's motion to quash, resting on the legal conclusion that an SCA warrant is more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it is stored at premises "owned, maintained, controlled, or operated by Microsoft Corporation." *In re Warrant*, 15 F. Supp. 3d at 468 (quoting Warrant). The fact that those premises were located abroad was, in the magistrate judge's view, of no moment. *Id.* at 472.

Microsoft offers a different conception of the reach of an SCA warrant. It understands such a warrant as more closely resembling a traditional warrant than a subpoena. In its view, a warrant issued under the Act cannot be given effect as to materials stored beyond United States borders, regardless of what may be retrieved electronically from the United States and where the data would be reviewed. To enforce the Warrant as the government proposes would effect an unlawful extraterritorial application of the SCA, it asserts, and would work an unlawful intrusion on the privacy of Microsoft's customer.

Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States. As to the citizenship of the customer whose

e-mail content was sought, the record is silent. For its part, the SCA is silent as to the reach of the statute as a whole and as to the reach of its warrant provisions in particular. Finally, the presumption against extraterritorial application of United States statutes is strong and binding. *See Morrison*, 561 U.S. at 255. In these circumstances, we believe we must begin our analysis with an inquiry into whether Congress, in enacting the warrant provisions of the SCA, envisioned and intended those provisions to reach outside of the United States. If we discern that it did not, we must assess whether the enforcement of this Warrant constitutes an unlawful extraterritorial application of the statute. We thus begin with a brief review of *Morrison*, which outlines the operative principles.

B. *Morrison* and the Presumption Against Extraterritoriality

When interpreting the laws of the United States, we presume that legislation of Congress "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. *Id*. at 255 (internal quotation marks omitted); *see also RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *7 (June 20, 2016). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." *Id*. The presumption reflects that Congress, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." *Equal Emp't Opportunity Comm'n v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991) ("*Aramco*"); *see generally Park Central Global Hub Ltd. v. Porsche Auto. Holdings SE*, 763 F.3d 198 (2d Cir. 2014) (per curiam).

To decide whether the presumption limits the reach of a statutory provision in a particular case, "we look to see whether 'language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control.'" *Aramco*, 499 U.S. at 248 (alteration in original) (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949)). The statutory provision must contain a "clear indication of an extraterritorial application"; otherwise, "it has none." *Morrison*, 561 U.S. at 255; *see also RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *7.

Following the approach set forth in *Morrison*, our inquiry proceeds in two parts. We first determine whether the relevant statutory provisions contemplate extraterritorial application. *Id*. at 261–65. If we conclude that they do not, by identifying the statute's focus and looking at the facts presented through that prism, we then assess whether the challenged application is "extraterritorial" and therefore outside the statutory bounds. *Id.* at 266–70.

C. Whether the SCA's Warrant Provisions Contemplate Extraterritorial Application

We dispose of the first question with relative ease. The government conceded at oral argument that the warrant provisions of the SCA do not contemplate or permit extraterritorial application.[19] Our review of the statute confirms the soundness of this concession.

[19] When asked, "What text in the Stored Communications Act do you point to, to support your assertion that . . . Congress intended extraterritorial application?", the government responded, "There's no extraterritorial application here at all." Recording of Oral Argument at 1:06:40–1:07:00. Later, when Judge Lynch observed, "I take it that suggests that the government actually agrees that there shall not be extraterritorial application of the Stored Communications Act . . . what this dispute is about is about the focus of the statute and what counts as an extraterritorial

Add. 23

1. Plain Meaning of the SCA

As observed above, the SCA permits the government to require service providers to produce the contents of certain priority stored communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a), (b)(1)(a). The provisions in § 2703 that permit a service provider's disclosure in response to a duly obtained warrant do not mention any extraterritorial application, and the government points to no provision that even implicitly alludes to any such application. No relevant definition provided by either Title I or Title II of ECPA, *see* 18 U.S.C. §§ 2510, 2711, suggests that Congress envisioned any extraterritorial use for the statute.

When Congress intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent. *Morrison*, 561 U.S. at 265. It did so, for example, in the statutes at issue in *Weiss v. National Westminster Bank PLC*, 768 F.3d 202, 207 & n.5 (2d Cir. 2014) (concluding that definition of "international terrorism" within 18 U.S.C. § 2331(1) covers extraterritorial conduct because Congress referred to acts that "occur primarily outside the territorial jurisdiction of the United States") and *United States v. Weingarten*, 632 F.3d 60, 65 (2d Cir. 2011) (concluding that 18 U.S.C. § 2423(b) applies to extraterritorial conduct because it criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors" that would violate United States law had the acts occurred in the jurisdiction of the United States). We see no such indication in the SCA.

---

application of the statute," the government answered, "That's right, Judge." *Id.* at 1:25:38–1:26:05.

We emphasize further that under § 2703, any "court of competent jurisdiction"—defined in § 2711(3)(B) to include "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants"—may issue an SCA warrant. Section 2703(a) refers directly to the use of State warrant procedures as an adequate basis for issuance of an SCA warrant. 18 U.S.C. § 2703(a). We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least "address[ing] the subject of conflicts with foreign laws and procedures." *Aramco*, 499 U.S. at 256; *see also American Ins. Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003) (describing as beyond dispute the notion that "state power that touches on foreign relations must yield to the National Government's policy").

The government asserts that "[n]othing in the SCA's text, structure, purpose, or legislative history indicates that compelled production of records is *limited* to those stored domestically." Gov't Br. at 26 (formatting altered and emphasis added). It emphasizes the requirement placed on a service provider to disclose customers' data, and the absence of any territorial reference restricting that obligation. We find this argument unpersuasive: It stands the presumption against extraterritoriality on its head. It further reads into the Act an extraterritorial awareness and intention that strike us as anachronistic, and for which we see, and the government points to, no textual or documentary support.[20]

[20] Seeking additional grounds for its position that to apply *Morrison* in this case is to proceed on a false premise, the government argues that the presumption against extraterritoriality applies only to "substantive provisions" of United States law, and that the SCA's warrant provisions are procedural. Gov't Br. at 31. The proposition that the SCA's protections are merely procedural might reasonably be questioned. But even assuming that they are procedural, the government gains no traction with this argument, which we rejected in *Loginovskaya v. Batratchenko*, 764 F.3d 266, 272-73 (2d Cir. 2014).

Add. 25

2. The SCA's Use of the Term of Art "Warrant"

Congress's use of the term of art "warrant" also emphasizes the domestic boundaries of the Act in these circumstances.

In construing statutes, we interpret a legal term of art in accordance with the term's traditional legal meaning, unless the statute contains a persuasive indication that Congress intended otherwise. *See F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'") (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). "Warrant" is such a term of art.

The term is endowed with a legal lineage that is centuries old. The importance of the warrant as an instrument by which the power of government is exercised and constrained is reflected by its prominent appearance in the Fourth Amendment to the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. It is often observed that "[t]he chief evil that prompted the framing and adoption of the Fourth Amendment was the indiscriminate searches and seizures conducted by the British under the authority of general warrants." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (internal quotation marks omitted). Warrants issued in accordance with the Fourth Amendment thus identify discrete objects and places, and restrict the government's ability to act beyond the warrant's

purview — of particular note here, outside of the place identified, which must be described in the document. *Id*. at 445–46.

As the term is used in the Constitution, a warrant is traditionally moored to privacy concepts applied within the territory of the United States: "What we know of the history of the drafting of the Fourth Amendment . . . suggests that its purpose was to restrict searches and seizures which might be conducted by the United States in domestic matters." *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008) (alteration omitted and ellipses in original) (quoting *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990)). Indeed, "if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation." *Id*. at 171. Accordingly, a warrant protects privacy in a distinctly territorial way.[21]

The SCA's legislative history related to its post enactment amendments supports our conclusion that Congress intended to invoke the term "warrant" with all of its traditional, domestic connotations.[22] Since the SCA's initial passage in 1986, Congress has amended § 2703 to relax some of the Rule 41 requirements as they relate to SCA warrants. Although some address the reach of SCA warrants, none of the amendments

---

[21] The government argues that the SCA's warrant provisions were "modeled after the Right to Financial Privacy Act," 12 U.S.C. §§ 3402(3), 3406, and that the latter act also "envisions that warrants—along with subpoenas and summonses—will trigger a disclosure requirement." Gov't Br. at 19 (citing S. Rep. No. 99-541, at 3). It points to no authority definitively construing the latter act's warrant provisions, however, nor any acknowledgment in the history of the SCA that enforcement of the warrant's disclosure commands would cross international boundaries. For these reasons, we accord little weight to the observation.

[22] We note that a 2009 amendment to Rule 41 expressly authorizes the use of such warrants to seize electronically-stored data, without abandoning the requirement that the warrant specify the place from which the data is to be seized. *See* Fed. R. Crim. P. 41(e)(2)(B) (allowing magistrate judge to "authorize the seizure of *electronic storage media* or the seizure or copying of *electronically stored information*" (emphasis added)).

contradicts the term's traditional domestic limits. *See* USA PATRIOT ACT, Pub. L. 107-56, § 220; 115 Stat. 272, 291–92 (2001) (codified at 18 U.S.C. § 2703(a), (b)); 21st Century Department of Justice Appropriations Authorization Act, Pub. L. 107-273, § 11010, 116 Stat. 1758, 1822 (2002) (codified at 18 U.S.C. § 2703(g)); Foreign Evidence Request Efficiency Act of 2009, Pub. L. 111-79, § 2, 123 Stat. 2086, 2086 (2009) (codified at 18 U.S.C. § 2711(3)(A)). These amendments to the SCA are fully consistent with the historical role of warrants as legal instruments that pertain to discrete objects located within the United States, and that are designed to protect U.S. citizens' privacy interests.

The magistrate judge took a different view of the legislative history of certain amendments to the SCA. He took special notice of certain legislative history related to the 2001 amendment to the warrant provisions enacted in the USA PATRIOT ACT. A House committee report explained that "[c]urrently, Federal Rules [*sic*] of Criminal Procedure 41 requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston . . . might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California." *In re Warrant*, 15 F. Supp. 3d at 473 (quoting H.R. Rep. 107-236(I), at 57 (2001)). The magistrate judge reasoned that this statement equated the location of property with the location of the service provider, and not with the location of any server. *Id.* at 474.

But this excerpt says nothing about the need to cross international boundaries; rather, while noting the "cross-jurisdictional nature of the Internet," it discusses only amendments to Rule 41 that allow magistrate judges "within the district" to issue warrants to be executed in other "districts"—not overseas. *Id.* at 473 (quoting H.R. Rep. 107-236(I), at 58). Furthermore, the Committee discussion reflects no expectation that the material to be searched and seized would be located any place other than where the

service provider is located. Thus, the Committee's hypothetical focuses on a situation in which an investigator in Boston might seek e-mail from "an Internet service provider (ISP) *account* located in California." To our reading, the Report presumes that the service provider is located where the account is—within the United States.[23]

3. Relevance of Law on "Subpoenas"

We reject the approach, urged by the government and endorsed by the District Court, that would treat the SCA warrant as equivalent to a subpoena. The District Court characterized an SCA warrant as a "hybrid" between a traditional warrant and a subpoena because—generally unlike a warrant—it is executed by a service provider rather than a government law enforcement agent, and because it does not require the presence of an agent during its execution. *Id*. at 471; 18 U.S.C. § 2703(a)-(c), (g). As flagged earlier, the subpoena-warrant distinction is significant here because, unlike warrants, subpoenas may require the production of communications stored overseas. 15 F. Supp. 3d at 472 (citing *Marc Rich*, 707 F.2d at 667).

Warrants and subpoenas are, and have long been, distinct legal instruments.[24] Section 2703 of the SCA recognizes this distinction and, unsurprisingly, uses the

[23] Our brief discussion here of the law of warrants is offered in aid only of our interpretation of the statutory language. Consequently, we do not consider whether the Fourth Amendment might be understood to impose disclosure-related procedural requirements more stringent than those established by the SCA. S*ee United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (finding Fourth Amendment protects certain electronic communications based on users' reasonable expectations of privacy); *see also* Email Privacy Act, H. R. 699, 114th Cong. § 3 (passed by House Apr. 27, 2016) (requiring government to obtain warrant before obtaining documents stored online).

[24] A "subpoena" (from the Latin phrase meaning "under penalty,") is "[a] writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply." *Subpoena,* Black's Law Dictionary. Relatedly, a "subpoena duces tecum" directs the person served to bring with him "specified documents, records, or things." *Subpoena duces*

"warrant" requirement to signal (and to provide) a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level. 18 U.S.C. § 2703(a), (b)(1)(A). Section 2703 does not use the terms interchangeably. *Id.* Nor does it use the word "hybrid" to describe an SCA warrant. Indeed, § 2703 places priority stored communications entirely outside the reach of an SCA subpoena, absent compliance with the notice provisions. *Id.* The term "subpoena," therefore, stands separately in the statute, as in ordinary usage, from the term "warrant." We see no reasonable basis in the statute from which to infer that Congress used "warrant" to mean "subpoena."

Furthermore, contrary to the Government's assertion, the law of warrants has long contemplated that a private party may be required to participate in the lawful search or seizure of items belonging to the target of an investigation. When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *Gambino v. United States*, 275 U.S. 310, 316–17 (1927); *see also Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006). The SCA's warrant provisions fit comfortably within this scheme by requiring a warrant for the content of stored communications even when the warrant commands a service provider, rather than a law enforcement officer, to access the communications. 18 U.S.C. § 2703(a), (b)(1)(A), (g). Use of this mechanism does not signal that, notwithstanding its use of the term

---

tecum, Black's Law Dictionary. In contrast, a "warrant" is a "writ directing or authorizing someone to do an act [such as] one directing a law enforcer to make . . . a search, or a seizure." *Warrant*, Black's Law Dictionary. As to search warrants, the place is key: A search warrant is a "written order authorizing a law-enforcement officer to conduct a search *of a specified place*." *Search Warrant*, Black's Law Dictionary.

"warrant," Congress intended the SCA warrant procedure to function like a traditional subpoena. We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application.

The government nonetheless urges that the law of subpoenas relied on by the magistrate judge requires a subpoena's recipient to produce documents no matter where located, and that this aspect of subpoena law should be imported into the SCA's warrant provisions. The government argues that "subpoenas, orders, and warrants are equally empowered to obtain records . . . through a disclosure requirement directed at a service provider." Gov't Br. at 18–19. It further argues that disclosure in response to an SCA warrant should not be read to reach only U.S.-located documents, but rather all records available to the recipient. *Id*. at 26–27.

In this, the government rests on our 1983 decision in *Marc Rich*. There, we permitted a grand jury subpoena issued in a tax evasion investigation to reach the overseas business records of a defendant Swiss commodities trading corporation. The *Marc Rich* Court clarified that a defendant subject to the personal jurisdiction of a subpoena-issuing grand jury could not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad." 707 F.2d at 667. The federal court had subject-matter jurisdiction over the foreign defendant's actions pursuant to the "territorial principle," which allows governments to punish an individual for acts outside their boundaries when those acts are "intended to produce and do produce detrimental effects within it." *Id.* at 666. In investigating such a case, the Court concluded, the grand jury necessarily had authority to obtain evidence related to the foreign conduct, even when that evidence was located abroad. *Id.* at 667. For that reason, as long as the Swiss corporation was subject to the grand jury's

personal jurisdiction—which the Court concluded was the case—the corporation was bound by its subpoena. *Id*. Thus, in *Marc Rich*, a subpoena could reach documents located abroad when the subpoenaed foreign defendant was being compelled to turn over its own records regarding potential illegal conduct, the effects of which were felt in the United States.

Contrary to the government's assertion, neither *Marc Rich* nor the statute gives any firm basis for importing law developed in the subpoena context into the SCA's warrant provisions. Microsoft convincingly observes that our Court has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.[25] Appellant's Br. at 42–43. The government does not identify, and our review of this Court's precedent does not reveal, any such cases.

The government also cites, and the District Court relied on, a series of cases in which banks have been required to comply with subpoenas or discovery orders requiring disclosure of their overseas records, notwithstanding the possibility that

[25] The government contends that Microsoft has waived the argument that the government cannot compel production of records that Microsoft holds on its customers' behalf. Gov't Br. at 36 & n.14. But in the District Court proceedings, Microsoft argued that there was a "difference between, on the one hand asking a company for its own documents . . . versus when you are going after someone else's documents . . . that are entrusted to us on behalf of our clients." Transcript of Oral Argument at 17, *In re Warrant*, 1:13-mj-02814, ECF No. 93. Although this was not the centerpiece of Microsoft's argument before the District Court, it was sufficiently raised. And in any event, we are free to consider arguments made on appeal in the interests of justice even when they were not raised before the district court. *See Gibeau v. Nellis*, 18 F.3d 107, 109 (2d Cir. 1994). The government has had an ample opportunity to rebut Microsoft's position, and we see no reason to treat this important argument as beyond our consideration.

compliance would conflict with their obligations under foreign law.[26] But the Supreme Court has held that bank depositors have no protectable privacy interests in a bank's records regarding their accounts. *See United States v. Miller*, 425 U.S. 435, 440–41 (1976) (explaining that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers"). Thus, our 1968 decision in *United States v. First National City Bank* poses no bar to Microsoft's argument. There, we held that a bank subject to the jurisdiction of a federal court was not absolutely entitled to withhold from a grand jury subpoena its banking records held in Frankfurt, Germany "relating to any transaction in the name of (or for the benefit of)" certain foreign customers solely because the bank faced the prospect of civil liability. 396 F.2d 897, 898, 901, 905 (2d Cir. 1968); *cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 101–02, 109 (2d Cir. 2013) (declining to issue writ of mandamus overturning district court's imposition of sanctions on foreign bank, when bank was civil defendant and refused to comply with discovery orders seeking certain foreign banking records).

We therefore conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially.

D. Discerning the "Focus" of the SCA

This conclusion does not resolve the merits of this appeal, however, because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Morrison*, 561 U.S. at 266. When we find that a law does

[26] Thus, in addition to *Marc Rich*, the government refers us to other cases that it characterizes as ordering production despite potential or certain conflict with the laws of other nations: *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817, 826–29 (11th Cir. 1984); *United States* v. *Vetco Inc.*, 691 F.2d 1281, 1287–91 (9th Cir. 1981); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 547, 564 (S.D.N.Y. 2002) (Chin, *J.*); *United States* v. *Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080, 1086–87 (S.D.N.Y. 1984). Gov't Br. at 16–17.

not contemplate or permit extraterritorial application, we generally must then determine whether the case at issue involves such a prohibited application. *Id* at 266–67. As we recently observed in *Mastafa v. Chevron Corp.*, "An evaluation of the presumption's application to a particular case is essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all." 770 F.3d 170, 182 (2d Cir. 2014).

In making this second-stage determination, we first look to the "territorial events or relationships" that are the "focus" of the relevant statutory provision. *Id*. at 183 (alterations and internal quotation marks omitted). If the domestic contacts presented by the case fall within the "focus" of the statutory provision or are "the objects of the statute's solicitude," then the application of the provision is not unlawfully extraterritorial. *Morrison*, 561 U.S. at 267. If the domestic contacts are merely secondary, however, to the statutory "focus," then the provision's application to the case is extraterritorial and precluded.

In identifying the "focus" of the SCA's warrant provisions, it is helpful to resort to the familiar tools of statutory interpretation, considering the text and plain meaning of the statute, *see, e.g.*, *Gottlieb v. Carnival Corp.*, 436 F.3d 335, 337 (2d Cir. 2006), as well as its framework, procedural aspects, and legislative history. *Cf. Morrison*, 561 U.S. at 266–70 (looking to text and statutory context to discern focus of statutory provision); *Loginovskaya*, 764 F.3d at 272–73 (analyzing text, context, and precedent to discern focus for *Morrison* purposes). Having done so, we conclude that the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content — the "object[] of the statute's solicitude." *Morrison*, 561 U.S. at 267.

Add. 34

1. The SCA's Warrant Provisions

The reader will recall the SCA's provisions regarding the production of electronic communication content: In sum, for priority stored communications, "a governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the rules described in the Federal Rules of Criminal Procedure," except (in certain cases) if notice is given to the user. 18 U.S.C. § 2703(a), (b).

In our view, the most natural reading of this language in the context of the Act suggests a legislative focus on the privacy of stored communications. Warrants under § 2703 must issue under the Federal Rules of Criminal Procedure, whose Rule 41 is undergirded by the Constitution's protections of citizens' privacy against unlawful searches and seizures. And more generally, § 2703's warrant language appears in a statute entitled the Electronic Communications Privacy Act, suggesting privacy as a key concern.

The overall effect is the embodiment of an expectation of privacy in those communications, notwithstanding the role of service providers in their transmission and storage, and the imposition of procedural restrictions on the government's (and other third party) access to priority stored communications. The circumstances in which the communications have been stored serve as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection they receive—in particular whether the Act's warrant provisions, subpoena provisions, or its § 2703(d) court order provisions govern a disclosure desired by the government. Accordingly, we think it fair to conclude based on the plain meaning of the text that the privacy of the stored communications is the "object[] of the statute's solicitude," and the focus of its provisions. *Morrison*, 561 U.S. at 267.

Add. 35

2. Other Aspects of the Statute

In addition to the text's plain meaning, other aspects of the statute confirm its focus on privacy.

As we have noted, the first three sections of the SCA contain its major substantive provisions. These sections recognize that users of electronic communications and remote computing services hold a privacy interest in their stored electronic communications. In particular, § 2701(a) makes it unlawful to "intentionally access[] without authorization," or "intentionally exceed[] an authorization to access," a "facility through which an electronic communication service is provided" and "thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." Contrary to the government's contention, this section does more than merely protect against the disclosure of information by third parties. By prohibiting the alteration or blocking of access to stored communications, this section also shelters the communications' integrity. Section 2701 thus protects the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties.

Section 2702 generally prohibits providers from "knowingly divulg[ing]" the "contents" of a communication that is in electronic storage subject to certain enumerated exceptions. 18 U.S.C. § 2702(a). Sections 2701 and 2702 are linked by their parallel protections for communications that are in electronic storage. Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government, creating the elaborate hierarchy of privacy protections that we have described.

From this statutory framework we find further reason to conclude that the SCA's focus lies primarily on the need to protect users' privacy interests. The primary obligations created by the SCA protect the electronic communications. Disclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in § 2703. Had the Act instead created, for example, a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest, the government's argument that the Act's focus is on aiding law enforcement and disclosure would be stronger. *Cf. Morrison*, 561 U.S. at 267. But this is not what the Act does.

The SCA's procedural provisions further support our conclusion that the Act focuses on user privacy. As noted above, the SCA expressly adopts the procedures set forth in the Federal Rules of Criminal Procedure. 18 U.S.C. § 2703(a), (b)(1)(A). Rule 41, which governs the issuance of warrants, reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy. *See* Fed. R. Crim. P. 41. Further, the Act provides criminal penalties for breaches of those privacy interests and creates civil remedies for individuals aggrieved by a breach of their privacy that violates the Act. *See* 18 U.S.C. §§ 2701, 2707. These all buttress our sense of the Act's focus.

We find unpersuasive the government's argument, alluded to above, that the SCA's warrant provisions must be read to focus on "disclosure" rather than privacy because the SCA permits the government to obtain by mere subpoena the content of e-mails that have been held in ECS storage for *more than* 180 days. Gov't Br. at 28–29; *see* 18 U.S.C. § 2703(a). In this vein, the government submits that reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers "beyond the reach of the statute entirely," while older e-mail content stored on foreign

servers could be obtained simply by subpoena, if notice is given to the user. Gov't Br. at 29. This argument assumes, however, that a subpoena issued to Microsoft under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers. Although our Court's precedent regarding the foreign reach of subpoenas (and *Marc Rich* in particular) might suggest this result, the protections rightly accorded user content in the face of an SCA subpoena have yet to be delineated. Today, we need not determine the reach of the SCA's subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant. Certainly, the service provider's role in relation to a customer's content supports the idea that persuasive distinctions might be drawn between it and other categories of subpoena recipients. *See supra* note 23.

In light of the plain meaning of the statutory language and the characteristics of other aspects of the statute, we conclude that its privacy focus is unmistakable.

3. Legislative History

We consult the Act's legislative history to test our conclusion.

In enacting the SCA, Congress expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications. *See* S. Rep. No. 99-541, at 3 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information."); H.R. Rep. No. 99-647, at 19 (1986) ("[M]ost important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."). In particular, Congress noted that the actions of private parties were largely unregulated when it came to maintaining the privacy of stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 18. And Congress observed further that recent Supreme Court precedent

called into question the breadth of the protection to which electronic records and communications might be entitled under the Fourth Amendment. *See* S. Rep. No. 99-541, at 3 (citing *United States v. Miller*, 425 U.S. 435 (1976), for proposition that because records and private correspondence in computing context are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection"); H.R. Rep. No. 99-647, at 23 (citing *Miller* for proposition that "under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services").

Accordingly, Congress set out to erect a set of statutory protections for stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 19. In regard to governmental access, Congress sought to ensure that the protections traditionally afforded by the Fourth Amendment extended to the electronic forum. *See* H.R. Rep. No. 99-647, at 19 ("Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment."). It therefore modeled § 2703 after its understanding of the scope of the Fourth Amendment. As the House Judiciary Committee explained in its report, it appeared likely to the Committee that "the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required." *Id.* at 22.

We believe this legislative history tends to confirm our view that the Act's privacy provisions were its impetus and focus. Although Congress did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment. *See* S. Rep. No. 99-541, at 3 (in drafting SCA, Senate Judiciary Committee sought "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs").

Taken as a whole, the legislative history tends to confirm our view that the focus of the SCA's warrant provisions is on protecting users' privacy interests in stored communications.

E. Extraterritoriality of the Warrant

Having thus determined that the Act focuses on user privacy, we have little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the Act. *See Morrison*, 561 U.S. at 266–67; *RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *9.

The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin. J.A. at 38. The record is silent regarding the citizenship and location of the customer. Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.[27] Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.[28] *Cf. Riley*

[27] We thus disagree with the magistrate judge that all of the relevant conduct occurred in the United States. *See In re Warrant*, 15 F. Supp. 3d at 475–76.

[28] The concurring opinion suggests that the privacy interest that is the focus of the statute may not be intrinsically related to the place where the private content is stored, and that an emphasis on place is "suspect when the content consists of emails stored in the 'cloud.'" Concurring Op. at 14 n.7. But even messages stored in the "cloud" have a discernible physical location. Here,

v. California, 134 S. Ct. 2473, 2491 (2014) (noting privacy concern triggered by possibility that search of arrestee's cell phone may inadvertently access data stored on the "cloud," thus extending "well beyond papers and effects in the physical proximity" of the arrestee).

The magistrate judge suggested that the proposed execution of the Warrant is not extraterritorial because "an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. . . . [I]t places obligations only on the service provider to act within the United States." *In re Warrant*, 15 F. Supp. 3d at 475–76. We disagree. First, his narrative affords inadequate weight to the facts that the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign. Second, the magistrate judge's observations overlook the SCA's formal recognition of the special role of the service provider vis-à-vis the content that its customers entrust to it. In that respect, Microsoft is unlike the defendant in *Marc Rich* and other subpoena recipients who are asked to turn over records in which only *they* have a protectable privacy interest.

The government voices concerns that, as the magistrate judge found, preventing SCA warrants from reaching data stored abroad would place a "substantial" burden on the government and would "seriously impede[]" law enforcement efforts. *Id*. at 474.

---

we know that the relevant data is stored at a datacenter in Dublin, Ireland. In contrast, it is possible that the identity, citizenship, and location of the user of an online communication account could be unknown to the service provider, the government, and the official issuing the warrant, even when the government can show probable cause that a particular account contains evidence of a crime.

The magistrate judge noted the ease with which a wrongdoer can mislead a service provider that has overseas storage facilities into storing content outside the United States. He further noted that the current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See* U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), *available at* fam.state.gov/FAM/07FAM/07FAM0960.html (last visited May 12, 2016) (discussing and listing MLATs).[29] And he observed that, for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad.[30]

These practical considerations cannot, however, overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of the term of art

---

[29] The United States has entered into an MLAT with all member states of the European Union, including Ireland. *See* Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.

[30] In addition, with regard to the foreign sovereign's interest, the District Court described § 442 (1)(a) of the Restatement of Foreign Relations Law as "dispositive." Tr. of Oral Arg., *supra* note 25, at 69. That section provides:

> A court or agency in the United States, when authorized by statute or rule of court, [is empowered to] order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.

Restatement of Foreign Relations Law (3d) § 442(1)(a) (1987). We are not persuaded. The predicate for the Restatement's conclusion is that the court ordering production of materials located outside the United States is "authorized by statute or rule of court" to do so. Whether such a statute—the SCA—can fairly be read to authorize the production sought is precisely the question before us.

"warrant," all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries. Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.

Thus, to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act.

CONCLUSION

We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland. Because Microsoft has otherwise complied with the Warrant, it has no remaining lawful obligation to produce materials to the government.

Add. 43

We therefore **REVERSE** the District Court's denial of Microsoft's motion to quash; we **VACATE** its order holding Microsoft in civil contempt of court; and we **REMAND** this cause to the District Court with instructions to quash the warrant insofar as it demands user content stored outside of the United States.

Add. 44

GERARD E. LYNCH, *Circuit Judge*, concurring in the judgment:

I am in general agreement with the Court's conclusion that, in light of the presumption against extraterritorial application of congressional enactments, the Stored Communications Act ("SCA" or the "Act") should not, on the record made by the government below, be construed to require Microsoft to turn over records of the content of emails stored on servers in Ireland. I write separately to clarify what, in my view, is at stake and not at stake in this case; to explain why I believe that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute.

I

An undercurrent running through Microsoft's and several of its amici's briefing is the suggestion that this case involves a government threat to individual privacy. I do not believe that that is a fair characterization of the stakes in this dispute. To uphold the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country.

As the majority correctly points out, the SCA presents a tiered set of requirements for government access to electronic communications and information relating to them. Although Congress adopted the Act in order to provide some privacy protections to such communications, *see* H.R. Rep. No. 99-647, at 21–23 (1986); S. Rep. No. 99-541, at 3 (1986), those requirements are in many ways less protective of privacy than many might think appropriate. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the SCA violates the Fourth Amendment to the extent that it allows government agents to obtain the contents of emails

without a warrant);[1] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004) (emphasizing that "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" and that "there are many problems of Internet privacy that the SCA does not address"). But this case does not require us to address those arguable defects in the statute. That is because in this case, the government complied with the most restrictive privacy-protecting requirements of the Act. Those requirements are consistent with the highest level of protection ordinarily required by the Fourth Amendment for the issuance of search warrants: a demonstration by the government to an independent judicial officer that evidence presented on oath justifies the conclusion that there is probable cause to believe that a crime has been committed, and that evidence of such crime can be found in the communications sought by the government.

That point bears significant emphasis. In this case, the government proved to the satisfaction of a judge that a reasonable person would believe that the records sought contained evidence of a crime. That is the showing that the framers of our Bill of Rights believed was sufficient to support the issuance of search warrants. U.S. Const. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . ."). In other words, in the ordinary domestic law enforcement context, if the government had made an equivalent showing that evidence of a crime could be found in a citizen's home, that showing would permit a judge to authorize law enforcement agents to forcibly enter that home and search every area of the home to locate the

[1] In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process. H.R. Rep. No. 114-528, at 9 (2016).

evidence in question, and even (if documentary or electronic evidence was sought) to rummage through file cabinets and to seize and examine the hard drives of computers or other electronic devices. That is because the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects" not absolutely, but only "against *unreasonable* searches and seizures," *id*. (emphasis added), and strikes the balance between the protection of privacy and the needs of law enforcement by requiring, in most cases, a warrant supported by a judicial finding of probable cause before the most intrusive of searches can take place. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2482 (2014).

Congress, of course, is free to impose even stricter requirements on specific types of searches – and it has occasionally done so, for example in connection with the real-time interception of communications (as in wiretapping and electronic eavesdropping). *See* 18 U.S.C. § 2518(3)(a) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes); *id*. § 2518(3)(c) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved). But it has not done so for permitting government access to any category of *stored* electronic communications, and Microsoft does not challenge the constitutional adequacy of the protections provided by the Act to those communications. Put another way, Microsoft does not argue here that, if the emails sought by the government were stored on a server at its headquarters in Redmond, Washington, there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case. Indeed, as explained above, the showing made by the government would support a warrant that permitted agents to forcibly enter those headquarters and seize the server itself.

I emphasize these points to clarify that Microsoft's argument is not that the government does not have sufficiently solid information, and sufficiently important interests, to justify invading the privacy of the customer whose emails are sought and acquiring records of the contents of those emails. Microsoft does not ask the Court to create, as a matter of constitutional law, stricter safeguards on the protection of those emails – and the Court does not do so. Rather, the sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing – in its own discretion – to store them on a server in another country.

That discretion raises another point about privacy. Under Microsoft's and the Court's interpretation of the SCA, the privacy of Microsoft's customers' emails is dependent not on the traditional constitutional safeguard of private communications – judicial oversight of the government's conduct of criminal investigations – but rather on the business decisions of a private corporation. The contract between Microsoft and its customers does not limit the company's freedom to store its customers' emails wherever it chooses, and if Microsoft chooses, for whatever reasons of profit or cost control, to repatriate the emails at issue here to a server in United States, there will be no obstacle to the government's obtaining them. As the Court points out, Microsoft does in fact choose to locate the records of anyone who *says* that he or she resides in the United States on domestic servers. It is only *foreign* customers, and those Americans who *say* that they reside abroad, who gain any enhanced protection from the Court's holding. And that protection is not merely enhanced, it is *absolute*: the government can never obtain a warrant that would require Microsoft to turn over those emails, however certain it may be that they

contain evidence of criminal activity, and even if that criminal activity is a terrorist plot.[2] Or to be more precise, the customer's privacy in that case is absolute *as against the government*; her privacy is protected against *Microsoft* only to the extent defined by the terms of her (adhesion) contract with the company.

Reasonable people might conclude that extremely stringent safeguards ought to apply to government investigators' acquisition of the contents of private email communications, and that the provisions of the SCA, as applied domestically, should be enhanced to provide even greater privacy, at an even higher cost to criminal investigations. Other reasonable people might conclude that, at least in some cases, investigators should have freer access to stored communications. It is the traditional task of Congress, in enacting legislation, and of the courts, in interpreting the Fourth Amendment, to strike a balance between privacy interests and law enforcement needs. But neither privacy interests nor the needs of law enforcement vary depending on whether a private company chooses to store records here or abroad – particularly when the "records" are electronic zeros and ones that can be moved around the world in seconds, and *will* be so moved whenever it suits the convenience or commercial purposes of the company. The issue facing the Court, then, is not actually about the need to enhance privacy protections for information that Americans choose to store in the "cloud."

---

[2] Although the Court does not reach the question, its opinion strongly suggests that that protection is absolute in the further sense that it applies also to less-protected categories of information otherwise reachable by the SCA's other disclosure-compelling instruments – subpoenas and court orders. If, as the Court holds, the "focus" of the SCA is privacy, and the relevant territorial locus of the privacy interest is where the customer's protected content is stored, *see* Majority Op. at 39, the use of the SCA to compel the disclosure of *any* email-related records stored abroad is impermissibly extraterritorial, regardless of the category of information or disclosure order.

II

In emphasizing the foregoing, I do not for a moment mean to suggest that this case is not important, or that significant non-privacy interests may not justify a congressional decision to distinguish records stored domestically from those stored abroad. It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. That question is important in its own right, and some further clarifications are in order about the division of responsibility between the courts and Congress in addressing it.

The courts have a significant role in the protection of privacy, because the Constitution sets limits on what even the elected representatives of the people can authorize when it comes to searches and seizures. Specifically, the courts have an independent responsibility to interpret the Fourth Amendment, an explicit check on Congress's power to authorize unreasonable searches. What searches are unreasonable is of course a difficult question, particularly when courts are assessing statutory authorizations of novel types of searches to deal with novel types of threat. In that context, courts need to be especially cautious, and respectful of the judgments of Congress. *See, e.g.*, *ACLU v. Clapper*, 785 F.3d 787, 824–25 (2d Cir. 2015). But it is ultimately the courts' responsibility to ensure that constitutional restraints on searches and seizures are respected.

Whether American law applies to conduct occurring abroad is a different type of question. That too is sometimes a difficult question. It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate

interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders.

But the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress. *See Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (Congress "alone has the facilities necessary to make fairly [the] important policy decision" whether a statute applies extraterritorially). No provision of the Constitution limits Congress's power to apply its laws to Americans, or to foreigners, abroad, and Congress has on occasion done so, expressly or by clear implication. The courts' job is simply to do their best to understand what Congress intended. Where Congress has clearly indicated that a law applies extraterritorially, as for example in 18 U.S.C. § 2332(a), which prohibits the murder of U.S. citizens abroad, the courts apply the law as written. *See RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *9–10 (June 20, 2016). We do the same when a law clearly applies only domestically.

The latter situation is far more common, so common that it is the ordinary presumption. When Congress makes it a crime to "possess a controlled substance," 21 U.S.C. § 844(a), it does not say that it is a crime to possess dangerous or addictive drugs *in the United States*. It speaks absolutely, as if proclaiming a universal rule, but we understand that the law applies only here; it does not prohibit the possession of marijuana by a Dutchman, or even by an American, in the Netherlands. "Congress generally legislates with domestic concerns in mind," *RJR Nabisco*, 2016 WL 3369423, at *8, quoting *Smith v. United States*, 507 U.S. 197, 204 n.5 (1993), and so,

unless Congress clearly indicates to the contrary, we presume that statutes have only domestic effect.

I have little trouble agreeing with my colleagues that the SCA does not have extraterritorial effect. As the Supreme Court recently made clear in *RJR Nabisco*, the presumption applies not only to statutes that straightforwardly regulate or criminalize conduct, but also to jurisdictional, procedural and remedial statutes. *Id.* at *15–16; *see also Loginovskaya v. Batratchenko*, 764 F.3d 266, 272 (2d Cir. 2014) (rejecting the argument that the presumption "governs substantive (conduct-regulating) provisions rather than procedural provisions"). Moreover, *RJR Nabisco* also reemphasized that the relevant question is not whether we think Congress "would have wanted" the statute to apply extraterritorially had it foreseen the precise situation before us, but whether it made clear its intention to give the statute extraterritorial effect. *RJR Nabisco*, 2016 WL 3369423, at *7. There is no indication whatsoever in the text or legislative history that Congress intended the Act to have application beyond our borders. It would be quite surprising if it had. The statute was adopted in the early days of what is now the internet, when Congress could hardly have foreseen that multinational companies providing digital services of all sorts would one day store vast volumes of communications and other materials for ordinary people and easily be able to move those materials across borders at lightning speed. *See* Majority Op. at 14.

The tricky part, in a world of transnational transactions taking place in multiple jurisdictions at once, is deciding whether a proposed application of a statute is domestic or extraterritorial. That determination can be complicated even for criminal acts when they touch on multiple jurisdictions, but the problem is particularly acute when we deal not with a simple

effort to regulate behavior that – given the physical limitations of human bodies – can often be fixed to a specific location, but with statutes that operate in more complex fashions. If SCA warrants were traditional search warrants, permitting law enforcement agents to search a premises and seize physical objects, the extraterritoriality question would be relatively easy: a warrant authorizing a search of a building physically located in Ireland would plainly be an extraterritorial application of the statute (and it would be virtually inconceivable under ordinary notions of international law that Congress would ever attempt to authorize any such thing). But as the government points out, this case differs from that classic scenario with respect to both the nature of the legal instrument involved and the nature of the evidentiary material the government seeks.

First, the "warrant" required for the government to obtain the emails sought in this case does not appear to be a traditional search warrant. Significantly, the SCA does not describe the warrant as a *search* warrant. Nor does it contain language implying (let alone saying outright) that the warrant to which it refers authorizes government agents to go to the premises of a service provider without prior notice to the provider, search those premises until they find the computer, server or other device on which the sought communications reside, and seize that device (or duplicate and "seize" the relevant data it contains).[3] Rather, the statute expressly

[3] I do note, however, that the particular warrant in this case states that the government "requests the search of" a "PREMISES" and "COMMAND[S]" an officer to "execute" the warrant on or before a certain date and time. J.A. 44. Neither party argues that this case turns on the language in the warrant itself, and the government explains that this language was included only because the warrant "was prepared using the generic template for search warrants." Gov't Br. 20. Nevertheless, it is worth emphasizing that the government itself chose the "template" it used to create the warrant it then asked the magistrate judge to sign. It is, to say the least, unimaginative for the government to utilize a warrant form that purports to authorize conduct that the statute under which it is obtained plainly does not permit, and then to turn around and

requires the "warrant" not to authorize a search or seizure, but as the procedural mechanism to allow the government to "require a [service provider] to disclose the contents of [certain] electronic communication[s]" *without notice to the subscriber or customer*. 18 U.S.C. § 2703(b)(1)(A). Parallel provisions permit the government to require equivalent disclosure of the communications by the service provider by a simple administrative subpoena or by a court order, provided only that notice is provided to the subscriber. *Id*. § 2703(b)(1)(B).[4] Indeed, the various methods of obtaining the communications, with or without notice, are not merely parallel – they all depend on the same verbal phrase. They are simply alternative means, applicable in different circumstances, to "require [the service provider] to disclose [the communications]." *Id*. § 2703(a), (b).

---

argue that this sort of warrant is completely different from what its language tells us it is, and that the language is unimportant because the government simply used the same formal template it uses under other, more traditional circumstances involving physical searches.

[4] One category of communications – those held "in electronic storage" by an electronic communication service for one hundred and eighty days or less – is reachable only by SCA warrant, with or without notice to the customer. 18 U.S.C. § 2703(a). But, although we ourselves have not addressed the issue, the majority view is that, once the user of an entirely web-based email service (such as Microsoft's) opens an email he has received, that email is no longer "in electronic storage" on an electronic communication service. *See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); *Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012); *id*. at 248 (Toal, C.J., concurring in the result); Kerr, *A User's Guide*, *supra*, at 1216–18 & n.61; *cf. Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 840–42 (8th Cir. 2015) (message retained on Gmail server in "sent" folder was not in electronic storage). *But see Cheng v. Romo*, Civ. No. 11-10007-DJC, 2013 WL 6814691, at *3–5 (D. Mass. Dec. 20, 2013); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); *cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1075–77 (9th Cir. 2003) (message is in electronic storage until it "has expired in the normal course"). Under that reading of the statute, only emails that have not yet been opened by the recipient fall into the category described above.

This difference is significant if we are looking to determine the "focus" of the SCA for purposes of determining whether a particular application of the statute is or is not extraterritorial. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 266–69 (2010). A search warrant "particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV, is naturally seen as focused on the *place* to be searched; as explained above, if the government argued that a statute authorized a search of a place outside the United States, that would clearly be an extraterritorial application of the statute. Here, however, the SCA warrant provision does not purport to authorize any such thing. Just like the parallel subpoena and court order provisions, it simply authorizes the government to *require the service provider to disclose* certain communications to which it has access.[5] The government quite reasonably argues that

[5] Although the Supreme Court has not addressed the question, there is considerable case law, including in this circuit, permitting the exercise of subpoena powers in precisely the situation in which the government demands records located abroad from an American company, or a foreign company doing business here. *See, e.g.*, *Linde v. Arab Bank, PLC*, 706 F.3d 92 (2d Cir. 2013); *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984); *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983); *United States v. First Nat'l City Bank*, 396 F.2d 897, 900–01 (2d Cir. 1968) ("It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."). At least as far as American courts are concerned (some foreign governments may think otherwise), such demands for the production of records are not seen as categorically impermissible extraterritorial uses of American investigatory powers, in the way that search warrants for foreign locations certainly would be. *Compare* Restatement (Third) of Foreign Relations Law § 442(1)(a) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.") *with id.* § 433(1) ("Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.").

Microsoft attempts to distinguish the cases cited above on the ground that the subpoenas in those cases required their recipients to disclose only the contents of their own business records, and not the records of a third party "held in trust" by the recipients. Appellant's Br. 48.

the focus of such a provision is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested.[6]

The nature of the records demanded is also relevantly different from that of the physical documents sought by traditional search warrants. Tangible documents, having a material existence in the physical world, are stored in a particular physical location. Executing a traditional search warrant requires a visit to that location, to visually inspect the documents to select the responsive materials and to take those materials away. Even when tangible documents are sought by subpoena, rather than by search warrant, it is arguable that the focus of the

---

"Email correspondance," Microsoft explains, is unlike bank records because it "is personal, even intimate," and "can contain the sum of an individual's private life." *Id*. at 44 (internal quotation marks omitted). Even assuming, however, that Microsoft accurately characterizes the cases it seeks to distinguish, *but cf. In re Horowitz*, 482 F.2d 72 (2d Cir. 1973) (partially upholding a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client), this privacy-based argument is, as explained above, a red herring. Microsoft does not dispute that the government could have required the disclosure of the emails at issue here if they were stored in the United States, and Microsoft's decision to store them abroad does not obviously entitle their owner to any higher degree of privacy protection.

[6] As the government notes, the selection of the term "warrant" to describe an instrument that does not operate like a traditional arrest or search warrant is easily explained by the fact that the provision in question, which permits government access to a person's stored communications without notice to that person, provides the highest level of privacy protection in the statute: the requirement that an independent judicial officer determine that probable cause exists to believe that a crime has been committed and that evidence of that crime may be found in the communications demanded. The *showing* necessary to obtain judicial authorization to require the service provider to disclose the communications is that associated with traditional warrants; the *manner* in which the disclosure is obtained by the government, however, is more closely analogous to the workings of subpoenas and court-ordered discovery: the government serves the service provider with an order from a court that requires the *service provider* to look within its records and *disclose* the specified information to the government; it does not present to the service provider a court order that permits *government agents* to search through the service provider's premises and documents and *seize* the specified information.

subpoena, for extraterritoriality purposes, is on the place where the documents are stored, since in order to comply with a subpoena seeking documents stored abroad, corporate employees will have to be present in the foreign location where the documents exist to inspect and select the relevant documents, which will then have to be transported out of that location and into the United States.

Electronic "documents," however, are different. Their location on a computer server in a foreign country is, in important ways, merely virtual. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408 (2014) (explaining that "the very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because computer files can be fragmented and dispersed across many servers). Corporate employees in the United States can review those records, when responding to the "warrant" or subpoena or court order just as they can do in the ordinary course of business, and provide the relevant materials to the demanding government agency, without ever leaving their desks in the United States. The entire process of compliance takes place domestically.

The government's characterization of the warrant at issue as domestic, rather than extraterritorial, is thus far from frivolous, and renders this, for me, a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute. One additional potential fact heightens the complexity. We do not know, on this record, whether the customer whose emails were sought by the government is or is not a United States citizen or resident. It is not clear that whether the customer is a United States person or not matters to the rather simplistic "focus" test adopted by the Supreme Court in *Morrison*, although it would have mattered to the more flexible test utilized by the Second Circuit in that case. *See Morrison v.*

Nat'l Australia Bank Ltd., 547 F.3d 167, 171 (2d Cir. 2008). But it seems to me that it *should* matter. The Supreme Court has rightly pointed out that the presumption against extraterritoriality is more than simply a means for avoiding conflict with foreign laws. *See Morrison*, 561 U.S. at 255. At the same time, the presumption that Congress legislates with domestic concerns pre-eminent in its collective mind does not fully answer the question what those domestic concerns are in any given case. *See id.* at 266. Particularly in connection with statutes that provide tools to law enforcement, one imagines that Congress is concerned with balancing liberty interests of various kinds against the need to enforce *domestic* law. Thus, when Congress authorizes the (American) government to obtain access to certain information, one might imagine that its focus is on balancing the liberty interests of *Americans* (and of other persons residing in the U.S.) against the need to enforce *American* laws. Congress might also reasonably be concerned about the diplomatic consequences of over-extending the reach of American law enforcement officials. This suggests a more complex balancing exercise than identifying a single "focus" of the legislation, the latter approach being better suited to determining whether given *conduct* fitting within the literal words of a prohibition should be characterized as domestic or extraterritorial.[7]

[7] While, for these reasons, it may be impossible to answer satisfactorily the question what the single focus of the SCA is, I note that I have considerable doubts about the answer supplied by the Court, which holds that the SCA provisions at issue here "focus on protecting the privacy of the content of a user's stored electronic communications." Majority Op. at 33. Privacy, however, is an abstract concept with no obvious territorial locus; the conclusion that the SCA's focus is privacy thus does not really help us to distinguish domestic applications of the statute from extraterritorial ones. "The real motor of the Court's opinion," *Morrison*, 561 U.S. at 284 (Stevens, *J.*, concurring in the judgment), then, is less the conclusion that the statute focuses on privacy than the majority's further determination that the locus of the invasion of privacy is where the private content is stored – a determination that seems to me suspect when the content consists of emails stored in the "cloud." It seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides.

Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part, and only in the interests of efficiency and good customer service) on local servers – and because the government did not include in its warrant application such information, if any, as it had about the target of its investigation – we do not know the nationality of the customer. If he or she is Irish (as for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland. The case looks rather different, however – at least to me, and I would hope to the people and officials of Ireland and the E.U. – if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company. Given that the extraterritoriality inquiry is essentially an effort to capture the congressional will, it seems to me that it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court.

These considerations give me considerable pause about treating SCA warrants as extraterritorial whenever the service provider from whom the government seeks to require

production has chosen to store the communications on a server located outside the United States. Despite that hesitation, however, I conclude that my colleagues have ultimately reached the correct result. If we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind in enacting the Act, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country. The use of the word "warrant" may not compel the conclusion that Congress intended to reach only domestically-stored communications that could be reached by a conventional search warrant, because, for the reasons given above, that label should not be controlling. *Cf. Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n*, 715 F.3d 631, 645–46 (7th Cir. 2013) (explaining that "we look to the substance of [the government's] inspection power rather than how the Act nominally refers to those powers," and holding that document requests under the Mine Safety and Health Act of 1977 should be treated as administrative subpoenas rather than as a search or seizure). But it is hard to believe that Congress would have used such a loaded term, and incorporated by reference the procedures applicable to purely domestic warrants, if it had given any thought at all to potential transnational applications of the statute. Nor is it likely that Congress contemplated such applications for a single moment. The now-familiar idea of "cloud" storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted. We should not lightly assume that Congress chose to permit SCA warrants for communications stored abroad when there is no sign that it considered the consequences of doing so. *See Kiobel*

v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013) ("The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches."). Thus, while I think the case is closer – and the government's arguments more potent – than is reflected in the Court's opinion, I come out in the same place.

III

Despite ultimately agreeing with the result in this case, I dwell on the reasons for thinking it close because the policy concerns raised by the government are significant, and require the attention of Congress. I do not urge that Congress write the government's interpretation into the Act. That is a policy judgment on which my own views have no particular persuasive force. My point is simply that the main reason that both the majority and I decide this case against the government is that there is no evidence that Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case. The SCA became law at a time when there was no reason to do so. But there is reason now, and it is up to Congress to decide whether the benefits of permitting subpoena-like orders of the kind issued here outweigh the costs of doing so.

Moreover, while I do not pretend to the expertise necessary to advocate a particular answer to that question, it does seem to me likely that a sensible answer will be more nuanced than the position advanced by either party to this case. As indicated above, I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely "domestic" statute. That may be the default position to which a court must revert in

the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness. Courts interpreting statutes that manifestly do not address these issues cannot easily create nuanced rules: the statute either applies extraterritorially or it does not; the particular demand made by the government either should or should not be characterized as extraterritorial. Our decision today is thus ultimately the application of a default rule of statutory interpretation to a statute that does not provide an explicit answer to the question before us. It does not purport to decide what the answer should be, let alone to impose constitutional limitations on the range of solutions Congress could consider.

Congress need not make an all-or-nothing choice. It is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of the corporate service provider. It could provide for access to such information only on a more demanding showing than probable cause, or only (as with wiretapping) where other means of investigation are inadequate, or only in connection with investigations into extremely serious crimes rather than in every law enforcement context. Or it could adopt other, more creative solutions that go beyond the possibilities evident to federal judges limited by their own experience and by the information provided by litigants in a particular case.

In addition, Congress need not limit itself to addressing the particular question raised by this case. The SCA was adopted in 1986, at a time when the kinds of services provided by "remote computing services" were not remotely as extensive and complex as those provided today, and when the economic and security concerns presented by such services were not remotely as important as they are now. More than a dozen years ago, a leading commentator was expressing the need to reform the Act. *See* Kerr, *A User's Guide*, *supra*, at 1233–42. It would seem to make sense to revisit, among other aspects of the statute, whether various distinctions, such as those between communications stored within the last 180 days and those that have been held longer, between electronic communication services and remote computing services, or between disclosures sought with or without notice to the customer, should be given the degree of significance that the Act accords them in determining the level of privacy protection it provides, or whether other factors should play some role in that determination.[8]

Congress has, in the past, proven adept at adopting rules for adapting the basic requirements of the Fourth Amendment to new technologies. The wiretapping provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–22, for example, proved to be a remarkably stable and effective structure for dealing with the privacy and law enforcement issues raised by electronic surveillance in the telephone era. More recently,

[8] As the Court notes, Majority Op. at 28 n.23, the House of Representatives recently passed a bill amending the SCA's required disclosure provisions. Email Privacy Act, H.R. 699, 114th Cong. § 3 (2016). That bill would require the government to obtain a warrant before it can compel the disclosure of the contents of any electronic communication "stored, held, or maintained" by either an electronic communication service or (under certain circumstances) a remote computing service, no matter the length of the period of storage. *Id*. It does not, however, address those provisions' extraterritorial reach or significantly modernize the statute's structure. *See* Kerr, *The Next Generation*, *supra*, at 386–89 (criticizing a proposal similar to the Email Privacy Act for "work[ing] within [the SCA's] outdated framework"). As of this writing, the Senate has not taken any action on the bill.

Congress was able to address the concerns presented by the mass acquisition of metadata by the National Security Agency by creating a more nuanced statute than that which the NSA had claimed as authority for its actions. *See ACLU v. Clapper*, 804 F.3d 617, 620 (2d Cir. 2015), discussing the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015). I fully expect that the Justice Department will respond to this decision by seeking legislation to overrule it. If it does so, Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs. Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations.

* * *

For these reasons, I concur in the result, but without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.